

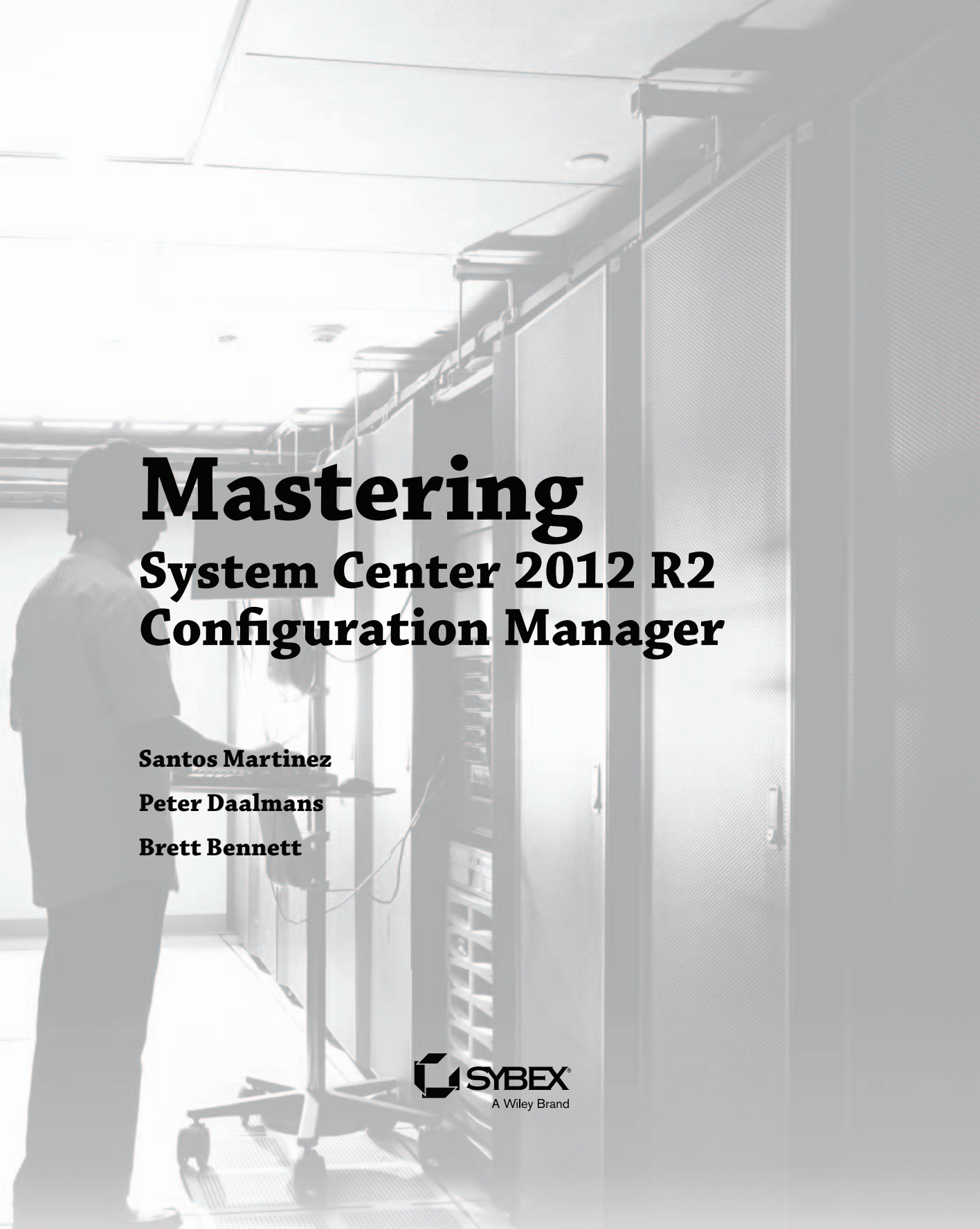
Santos Martinez
Peter Daalmans
Brett Bennett

Mastering System Center 2012 R2 Configuration Manager

SYBEX
A Wiley Brand



Mastering
System Center 2012 R2 Configuration Manager



Mastering
System Center 2012 R2 Configuration Manager

Santos Martinez

Peter Daalmans

Brett Bennett

SYBEX®
A Wiley Brand

Acquisitions Editor: Mariann Barsolo
Development Editor: Kim Wimpsett
Technical Editor: Don Brown
Production Editor: Dassi Zeidel
Copy Editor: Linda Recktenwald
Editorial Manager: Pete Gaughan
Vice President and Executive Group Publisher: Richard Swadley
Associate Publisher: Chris Webb
Book Designers: Maureen Forys, Happenstance Type-O-Rama; Judy Fung
Proofreader: Rebecca Rider
Indexer: Ted Laux
Project Coordinator, Cover: Todd Klemme
Cover Designer: Wiley
Cover Image: ©Getty Images, Inc./Thomas Northcutt

Copyright © 2014 by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-118-82170-1
ISBN: 978-1-118-82185-5 (ebk)
ISBN: 978-1-118-82173-2 (ebk)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at `http://www.wiley.com/go/permissions`.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at `http://booksupport.wiley.com`. For more information about Wiley products, visit `www.wiley.com`.

Library of Congress Control Number: 2013958294

TRADEMARKS: Wiley and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *Mastering System Center 2012 R2 Configuration Manager*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `contactus@sybex.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,



Chris Webb
Associate Publisher
Sybex, an Imprint of Wiley

I dedicate this book to my sister, Yolimar Martinez; it has been three years since you left the physical world, but I know you are in peace and have started a new journey. Also I want to dedicate this book to the following: my wife, Karla, you are my soul mate and I want to grow old with you; to my kids, Bryan and Naomy, I hope this gives you some inspiration one day of what you can possibly achieve, and finally to all my family and friends for their support in my craziness.
—Santos Martinez

I dedicate this book to my father; after 15 years, you are still deeply missed. To my mother, for all of your love and support in my life. To my girlfriend, Samantha, and our son, Stef; thanks for putting up with me and for all of your love and support while writing this book.
—Peter Daalmans

I dedicate this book to my family and friends, and I greatly appreciate the support you provide.
—Brett Bennett

Acknowledgments

There are so many people I have to thank. I will start by giving a big thank-you to my wife for supporting me all the time on this special project. I love you for that and many other things. I want to thank my colleagues across Microsoft for their support on this book like crazy; to our technical editor, Don Brown, you have done a great job making this book better and taking it to the next step. To the contributing authors, Kevin Robinson, Carlos Santiago, and Ramon Martinez, thanks for leaving a piece of yourselves in the book.

To my peer authors, Brett Bennett and Peter Daalmans, thanks for staying on the project and giving it your best; I know the readers will enjoy learning from both of you, and I had an amazing experience.

To my friend, Elias Mereb, for always delivering a great elevator pitch on the previous edition of the book; I look forward to hearing your stories on this book, too.

Finally, I want thank the entire ConfigMgr community, who have always been so passionate about the technology and willing to help us improve our writing. Let's keep the conversation going and going.

—Santos Martinez

Special thanks to my family and friends. I had to balance my time with you with my commitment to writing six chapters for this book. I couldn't have done this without you guys!

I also want to thank Wiley/Sybex for giving me the opportunity to write this second book. It was again a great pleasure to work with the Wiley team; I'm looking forward to any new project! Also, many thanks to the writing and editorial teams, you all rock!

Furthermore, many thanks to the Configuration Manager product team, who created this great product, and Wally Mead especially, our great and dedicated MVP lead from within the product team. They all give us the opportunity to learn as much as we want about Configuration Manager.

Also special thanks to my employers, Marco and Koos from IT-Concern, for giving me the space to speak at conferences and to be of value to the community.

In 2013 I had the honor to speak at TechEd Australia and TechEd New Zealand; besides Microsoft Australia and Microsoft New Zealand, I would like to thank my fellow Enterprise Client Management MVPs Kent Agerlund and James Bannan for their support Down Under.

Finally, many thanks to the Configuration Manager community and in particular all my fellow Enterprise Client Management MVPs; thanks for your support.

—Peter Daalmans

I would like to thank my wife, Rosalie, and my children, Brittany, Jamie, and Justin, for the support they have provided me in my career. I would also like to thank Microsoft Corporation, both as my employer for the past 7 years and for the amazing products they develop that have kept me gainfully employed for the past 25 years. I would like to thank the co-authors, reviewers, and the entire team at Sybex/Wiley who helped put this book together.

—Brett Bennett

About the Authors

Santos Martinez was born in Caguas, Puerto Rico, in 1982, and grew up in Caguas. Santos has more than 12 years of experience in the IT industry. He has worked on major implementations and in support of ConfigMgr and SMS migrations for financial institutions in the United States and Puerto Rico. Santos was a senior Configuration Manager engineer for a Fortune 500 financial institution and an IT consultant before joining Microsoft. For the Fortune 500 company, he helped with the implementation and support of more than 200 ConfigMgr servers and the support of more than 165 clients worldwide. After completing this project he did IT consulting work for many other corporations that were implementing ConfigMgr.

Santos was a SQL Server MVP from 2005 to 2009 and then a ConfigMgr MVP from 2009 to 2011. He is well-known in the Microsoft LATAM communities as a mentor for other MVPs and for helping other IT community members. He has also participated in Microsoft Tech Ed and Microsoft MMS as a technical expert for SMS/ConfigMgr. Santos is also a former Puerto Rican martial arts champion and currently holds a fourth-degree black belt in TaiFu Shoi Karate Do.

Santos and Karla, a pastry chef, have been married for 11 years and have two kids, Bryan Emir and Naomy Arwen.

Santos currently is a senior premier field engineer for Microsoft in the eastern region of the United States.

You can get in touch with Santos via his Twitter account `@ConfigNinja` or his blog `http://aka.ms/ConfigNinja`.

Peter Daalmans is a senior technical consultant at IT-Concern, a Gold Certified Microsoft Partner in the Netherlands. Peter was named an Enterprise Client MVP in 2012 and 2013 for his work in the community. Peter has worked with deployment tooling from Microsoft competitors since 1998; in 2005 Peter discovered BDD and SMS 2003 deployment tooling and has embraced them ever since. In recent years numerous international deployment projects have crossed Peter's path.

Peter is one of the founders of the Windows Management User Group Netherlands and shares his Configuration Manager and Windows Intune experience with the community via his blog (`http://ConfigMgrBlog.com`).

Besides speaking at the Windows Management User Group Netherlands, a couple of times a year Peter speaks at conferences like TechDays Netherlands and Experts Live, and in 2013 Peter had the opportunity to speak at TechEd Australia and TechEd New Zealand.

Peter resides in Breda, in the south of the Netherlands, with his girlfriend, Samantha, and his son, Stef. In addition to his daily work, he is the chairman of the NAC Museum Foundation, which preserves the history of the soccer club NAC Breda. Australia is also a huge passion; he travels Down Under whenever he gets the chance to sniff the outback and the Aussie lifestyle.

You can reach Peter via `@pdaalmans` and `peter@ConfigMgrBlog.com`.

Brett Bennett is a senior premier field engineer at Microsoft and has been working with SMS/ConfigMgr since SMS 1.0. Brett lives in Texas with his wife, Rosalie, and has three children. His daughter, Brittany, and his two sons, Jamie and Justin, all attend Texas A&M University in College Station (GIG 'EM!). Rosalie recently graduated from Texas A&M University-Commerce with a bachelor of science in history, and will soon fulfill her dream of becoming a high school history teacher. The Bennetts have three dogs: two black labs (Yogi and Boo Boo) and a golden retriever (Reeses) and also a granddog (Rue). Brett's hobbies include playing guitar, learning to play banjo, cycling, tinkering with his Dodge Challenger, and watching movies in his home theater.

About the Contributing Authors

Carlos Santiago is a senior premier field engineer at Microsoft. He has been working with Systems Management Server/Configuration Manager since version 1.0. He moved from Puerto Rico to Texas in 1992 and lives with his two sons, Christian and Zachary. Christian is a sophomore studying aerospace engineering at the University of Texas in Arlington, and Zachary can't wait to be in high school next year. The family enjoys the company of Crystal, a miniature Schnauzer dog, and Maximus, an Egyptian Mau cat. Carlos volunteers part of his free time to the Boy Scouts of America. Carlos's hobbies include electronics, shooting sports, photography, and camping.

Ramon Martinez is a premier field engineer at Microsoft and has been working with SMS/ConfigMgr since SMS 1.1. Ramon lives in Toronto, Ontario, Canada, with his abundant Latin family, including Sonia, Ramsoni, Natali, and Iris. All of his daughters have completed a higher education program. Natali graduated with honors and received a Canadian Broadcasting Corporation (CBC) Journalism award. Ramon's family also includes a dog pet. Ramon's hobbies include dancing salsa, bachata, merengue, and reaggeaton as well as alpine skiing. And of course Ramon is highly passionate about Spanish League Soccer. Ramon follows La Liga de Futbol, especially Real Madrid Club de Futbol.

Kevin Robinson is a senior premier field engineer at Microsoft and was formerly an Exin-certified ITIL service manager. He has also served as a principle service engineer in Microsoft's BPOS cloud service operations team. His lovely wife of 33 years, Patrice, and Kevin reside in Charlotte, North Carolina, where they enjoy travel, food, and entertaining friends and family. They are the proud parents of three sons, Myles, Dexter, and Jordan, who all attended North Carolina universities, along with their daughters-in-law Tiffany and Vanessa. Most recently Kevin and Patrice were blessed with their first grandchild, a precious little girl named Zoe Sanaa.

Contents at a Glance

Introduction . . . . . *xxiii*

Chapter 1 • Overview of Service Management 1

Chapter 2 • Planning a Configuration Manager Infrastructure 21

Chapter 3 • Migrating to Configuration Manager 2012 65

Chapter 4 • Installation and Site Role Configuration 121

Chapter 5 • Cloud Integration 213

Chapter 6 • Client Installation 227

Chapter 7 • Client Health 273

Chapter 8 • Application Deployment 291

Chapter 9 • Software Updates 363

Chapter 10 • Operating System Deployment 451

Chapter 11 • Inventory and Software Metering 527

Chapter 12 • Asset Intelligence 563

Chapter 13 • Reporting 583

Chapter 14 • Compliance Settings 623

Chapter 15 • System Center Endpoint Protection 669

Chapter 16 • Mobile Device Management 701

Chapter 17 • Role-Based Administration 773

Chapter 18 • Disaster Recovery 797

Chapter 19 • Troubleshooting 827

Appendix • The Bottom Line 861

Index *883*

Contents

Introduction . . . . . *xxiii*

Chapter 1 • Overview of Service Management 1

Understanding IT Service Management 1
Exploring the IT Infrastructure Library 2
Select ITIL Functions and Processes 5
Exploring the Microsoft Operations Framework 9
Select MOF Service Management Functions 10
Overview of System Center Configuration Manager 12
Configuration Manager Features 12
Summary 20

Chapter 2 • Planning a Configuration Manager Infrastructure 21

Gathering Deployment Intelligence 21
Determining What You Need to Accomplish 22
Describing the Network 23
Describing Your Migration Needs 23
Planning the Configuration Manager Environment 24
System Requirements 24
Extending the Active Directory Schema 37
Hierarchies and Sites 38
Site Boundaries and Boundary Groups 44
Site System Roles 45
Best Practices for Site System Design 47
SQL Considerations 49
Site Communications 50
Site Security Mode 51
Discovery of Your Resources 51
Client Settings and Client Deployment 52
Content Management 52
Role-Based Administration 53
Migration 54
Disaster Recovery 56
Designing Your Configuration Manager Environment 56
Planning the Configuration Manager Hierarchy 58
Planning Configuration Manager Site Systems 59
Planning Configuration Manager Clients 59
Determining How to Deploy Configuration Manager 60
Building a Proof-of-Concept Environment 60
The Bottom Line 64

Chapter 3 • Migrating to Configuration Manager 2012 65
Introducing Migration. 66
Migration Functionality in Configuration Manager 2012 67
Source Hierarchy 67
Data-Gathering Process 68
Migration Job Types 68
Objects Not Supported for Migration 79
Distribution Point Sharing 79
Planning a Migration. 80
Preparing Your Migration 81
Planning Your Migration Strategy. 81
Performing the Migration. 83
Using the Side-by-Side Migration Strategy. 83
Using the Wipe-and-Load Strategy 100
Upgrading the Configuration Manager Console. 100
Post-Migration or Installation Considerations. 101
Migrating Packages to the New Application Model. 103
What Is Package Conversion Manager? 103
The Conversion Process. 104
The Conversion Process Steps. 109
Package Conversion Manager Best Practices 110
Monitoring Conversion 110
Migrating Branch Offices with the Physical-to-Virtual Migration Toolkit. 111
Requirements. 112
P2V Migration Scenario 112
The Task Sequence 113
Steps for Using the Configuration Manager 2012 P2V Migration Toolkit 113
The Bottom Line. 120

Chapter 4 • Installation and Site Role Configuration 121
Understanding Configuration Manager 2012 R2 Site Types. 122
Implementing Site Servers 125
Software Requirements 125
Implementing a Central Administration Site. 127
Implementing a Primary Site 136
Implementing a Secondary Site 140
Verifying Proper Site Installation. 147
Troubleshooting a Configuration Manager 2012 R2 Site Installation. 154
Unattended Installation. 157
Installing Site System Roles 160
Understanding Configuration Manager 2012 R2 Site System Roles 163
Component Server 165
Distribution Point 165
Management Point 178
Site Database Server 183
Site Server. 184
Site System 184
System Health Validator Point 184
State Migration Point 186

Fallback Status Point 189
Out of Band Service Point 191
Reporting Services Point 193
Application Catalog Web Service Point and Application Catalog Website Point 195
Enrollment Point and Enrollment Proxy Point 199
Software Update Point 203
Endpoint Protection Point 209
Asset Intelligence Synchronization Point 210
The Bottom Line 212

Chapter 5 • Cloud Integration 213
Windows Azure Integration 214
Management Certificate for Site Server to Distribution Point Communication . . . 215
Creating a Cloud Distribution Point 215
Creating and Exporting the Management Certificate 216
Creating the Service Certificate Template 219
Requesting and Exporting the Service Certificate 220
Uploading the Management Certificate to Windows Azure 222
Creating the Cloud Distribution Point 222
Configure Name Resolution for Cloud-based Distribution Points 225
The Bottom Line 225

Chapter 6 • Client Installation 227
Creating Client Settings 227
Supported Operating Systems 232
Discovering Network Objects 234
Active Directory Discovery Methods 235
Configuring Boundaries and Boundary Groups 244
Client Installation Methods 247
Command-Line Properties 247
Manually Installing the Client 252
Client Push 253
Group Policy 257
Software Update 257
Software Distribution 258
Logon Script Installation 258
Imaging 258
Installing Linux/Unix Clients 259
Installing a Mac Client 262
Verifying Client Installation 265
Troubleshooting a Client Installation 266
Ensuring Client Health 266
Automatic Client Remediation 266
Determining Client Health 267
Monitoring Client Status 268
Configuring Alerts 268
Automatic Client Upgrade 270
The Bottom Line 271

Chapter 7 • Client Health 273
Understanding the Client Health Mechanism 273
Scheduled Task 274
CCMEval Process 279
Client Health Evaluation: Results 283
Configuring Client Health 284
Monitoring: Client Status 286
Alert: Client Health 287
The Bottom Line 289

Chapter 8 • Application Deployment 291
What's New in Application Deployment? 291
Distribution Point Changes 293
Applications: Application References 296
Deployments 296
Dependencies for Application Deployment 299
Management Point 299
Distribution Point 299
Default Client Settings 300
Elements of Application Deployment 308
Applications 308
Deployment Types 308
Deployments 310
The Application Deployment Process 310
Create Application Wizard 311
Creating an Application with PowerShell 314
Options for Application Deployment: the Ribbon 314
Exploring the Sample Application 319
Exploring the Deployment Type 323
Create Deployment Wizard 333
Application Deployment—Client Experience 339
Application Deployment—Advanced Configurations 343
User Device Affinity 355
Troubleshooting Application Deployment 358
The Bottom Line 361

Chapter 9 • Software Updates 363
What's New in Software Updates 364
Prerequisites for Software Updates 366
Elements of Software Updates 367
Software Update Point 367
Software Updates Agent 368
Software Updates Metadata 368
Software Update Files 369
Software Update Objects 369
Software Update Groups 371
Deployment Templates 371

Deployment Packages 372
Deployments 373
Automatic Deployment Rules 374
System Center Updates Publisher 376
The Software Update Process in Configuration Manager 376
Synchronization 376
Compliance 377
Deployment 378
Planning to Use Software Updates in Configuration Manager 380
Determining What Needs to Be Accomplished 380
Role-Based Administration 393
System Center Updates Publisher 394
Testing in an Isolated Lab 395
Configuring Software Updates 396
Configuring the Software Updates Client Agent 396
Installing Windows Server Update Services 3.0 Server 398
Installing the Windows Server Update Services 3.0 SP2 Administrative Console 402
Setting Up the Software Update Point 402
Configuring Software Updates Settings and Synchronization 414
Synchronizing Updates with Export and Import 418
Preparing Software Updates for Deployment 419
Finding the Software Updates to Be Deployed 420
Downloading Software Updates 424
Creating a Software Update Group 427
Deploying Software Updates with the Deploy Software Updates Wizard 427
Using System Center Updates Publisher 436
Installing System Center Updates Publisher 436
Configuring System Center Updates Publisher 436
Using System Center Updates Publisher 438
Third-Party Updates in Configuration Manager 443
Monitoring Software Update Deployments 445
In-Console Monitoring 445
Reporting 448
The Bottom Line 450

Chapter 10 • Operating System Deployment 451
What's New in Operating System Deployment 451
Planning for OSD with Configuration Manager 2012 452
Deployment Scenarios 452
The Kind of Images to Deploy 452
Operating System Deployment Components 453
User Device Affinity 459
Deployment Process 460
Prepare for Operating System Deployment 460
Build and Capture an Operating System 460
Deploy an Operating System 460

Preparing Configuration Manager 2012 for Operating System Deployment 461
Configuring the Network Access Account 461
Configuring the State Migration Point Role 462
Configuring PXE on Distribution Points 464
Distributing the Boot Image Package 466
Enabling Boot Images for PXE 467
Adding Operating System Source 468
Developing a Task Sequence for Creating a Capture Image 471
Task Sequences Used with PXE Boot 471
Task Sequences Used with Media Boot 475
Capturing an Operating System Image 477
Building and Capturing Automatically 477
Capturing a Reference Computer 480
Deploying an Image 482
Adding a Captured Image 482
Distributing and Deploying the Image 483
Developing a Task Sequence for Deployment 483
Deploying the Task Sequence 487
Deploying the Operating System on Bare Metal 492
Importing Computer Information 492
Creating a Task Sequence for the Bare-Metal OSD 493
Deploying the Bare-Metal Task Sequence 494
Installing Device Drivers into OSD 497
Using User Device Affinity 500
Manually Configure a Primary User for a Device 500
Manually Configure a Primary Device for a User 501
Configure a Site to Automatically Create User Device Affinities 501
Import User Device Affinities 502
Enable Users to Configure Their Primary Device 503
Pre-deploy User Applications 503
Deploying Windows To Go 504
Creating a Prestaged Media for the Task Sequence 504
Creating a Windows To Go Creator Package 506
Update the Task Sequence to Enable BitLocker 507
Running the Windows To Go Package 509
Microsoft Deployment Toolkit 2013 510
Installing Microsoft Deployment Toolkit 2013 510
Integrating the Deployment Toolkit 511
Creating a New Boot Image 512
Creating a Deployment Toolkit Task Sequence 513
Using a Replace Scenario 515
Deploying a Virtual Hard Drive 516
Creating a VHD Task Sequence 516
Creating a Virtual Hard Disk 517
Managing the Virtual Hard Disk 519
Servicing Your Operating System Images and VHDs Offline 520
Support for Legacy Boot Images 522
Maintaining the User State 524
The Bottom Line 525

Chapter 11 • Inventory and Software Metering 527
Inventory in Configuration Manager 2012 527
Collecting Hardware Inventory 528
Collecting Software Inventory 533
Using Resource Explorer to View Inventory 535
Scheduling Inventory 536
Configuring Inventory 537
Configuring Software Inventory for a Configuration Manager Site 542
Troubleshooting Inventory 550
Software Metering in Configuration Manager 2012 553
Overview of Software Metering 553
Configuring Software Metering 553
The Bottom Line 562

Chapter 12 • Asset Intelligence 563
Requirements for Asset Intelligence 563
Client Agent Prerequisites 564
Maintenance Tasks 564
Windows Ekvent Log Settings 565
Elements of Asset Intelligence 566
Asset Intelligence Catalog 566
Asset Intelligence Validation States 568
Asset Intelligence Synchronization Point 569
The Asset Intelligence Home Page 569
Asset Intelligence Reports 571
Configuring Asset Intelligence 575
Enabling Asset Intelligence 575
Import Software License into Asset Intelligence 578
Importing Software License Information 579
Creating the Microsoft Volume License Statement 579
Creating the General License Statement 580
The Bottom Line 581

Chapter 13 • Reporting 583
Installing SQL Server Reporting Services 584
Considerations for Installing SQL Server Reporting Services 585
Installation of the Reporting Services Site System 586
Default Reports 590
Running a Report 593
Viewing Available Reports 593
Running a Report from the Administrative Console 593
Running a Report from Report Manager 594
Working with Reporting Security 596
Permissions Required to Run Reports 596
Managing Reports 601
Working with Subscriptions 609
Creating Reports 611
Basic SQL Commands 612

Report Models 613
Creating a Report Using Report Builder 613
Creating a Report Using Business Intelligence Development Studio 616
Moving Reports 619
Linked Reports 619
Importing and Exporting Reports 620
Importing Reports 620
Exporting Reports 621
The Bottom Line 621

Chapter 14 • Compliance Settings 623

Overview of Compliance Settings 623
What's New in Configuration Manager 2012 R2? 624
What Can You Do with Compliance Settings? 625
Configuration Items 625
Configuring Compliance Settings Client Settings 627
Creating Configuration Items 628
Name, Description, and Category 629
Choosing a Detection Method 631
Creating and Validating a Setting 632
Building a Configuration Baseline 639
Creating the Initial Baseline 639
Baseline Rules 640
Assigning the Configuration Baseline to Clients 643
Additional Configuration Baseline Options 644
Client Validation of Compliance Baseline Rules 644
Compliance Settings Reporting 646
Importing Configuration Packs 647
User Data and Profiles 650
Remote Connection Profiles 654
Company Resource Access 656
Certificate Profiles 656
VPN Profiles 660
Wi-Fi Profiles 665
The Bottom Line 668

Chapter 15 • System Center Endpoint Protection 669

Differences between FEP and SCEP 669
Additional Benefits of SCEP 670
Deployment 670
Protection 670
Monitoring 672
Security 672
Endpoint Protection Site System Role 672
Endpoint Protection Client Agent 675
Endpoint Protection Policies 679
Antimalware Policy 679

Windows Firewall Policy . . . 685
Assigning Policy . . . 687
Definition Files . . . 687
Alerts . . . 690
Reporting . . . 693
Client Notifications . . . 694
The Bottom Line . . . 699

Chapter 16 • Mobile Device Management . . . 701

What's New in Mobile Device Management . . . 701
Mobile Device Management Options . . . 702
Lite Management . . . 705
Depth Management via Client . . . 715
Depth Management via Windows Intune . . . 728
Managing Mobile Devices . . . 742
Device Settings Management . . . 742
Wipe vs. Selective Wipe . . . 769
Troubleshooting . . . 771
The Bottom Line . . . 772

Chapter 17 • Role-Based Administration . . . 773

Overview of Role-Based Administration . . . 773
Using Security Roles and Security Scopes . . . 774
Managing with Flat Hierarchies . . . 774
Security Roles . . . 774
Security Scopes . . . 778
Creating a Custom Security Scope . . . 779
Assigning Resources to a Security Scope . . . 781
Viewing Security Scope Objects . . . 783
Collections . . . 784
Using Collections . . . 784
Understanding the Default Collections . . . 785
Administrative Users . . . 785
RBA Viewer . . . 793
The Bottom Line . . . 795

Chapter 18 • Disaster Recovery . . . 797

Planning for Disaster Recovery . . . 797
What Is Not Included in the Backup . . . 798
Backing Up Configuration Manager . . . 801
Backup Considerations for the Central Administration Site . . . 801
Copying Site Backups to Another Location . . . 802
Archiving the Backup Snapshot to Another Server with *AfterBackup.bat* . . . 802
Windows Application Log Entries Created by the Backup Process . . . 804
Configuring the Backup ConfigMgr Site Server Maintenance Task . . . 805
Restoring Configuration Manager . . . 807
Understanding the Effects of a Site Failure . . . 808
Recovering a Configuration Manager Site . . . 809

Recovering Configuration Manager 811
How to Start a Recovery Process 811
Recovering a Central Administration Site 811
Recovering a Primary Child Site 817
Recovering a Primary Standalone Site 817
Recovering a Secondary Site 818
Recovery Scenarios for Multisite Environments 818
Unattended Recovery of a Site 818
Other Site Maintenance Options 819
The Hierarchy Maintenance Tool 819
Post-Recovery Tasks 821
The Bottom Line 824

Chapter 19 • Troubleshooting 827
Creating the Maintenance Plan 827
Using Troubleshooting Tools 832
Log Files 832
Status Messages 837
Troubleshooting Configuration Manager Deployment 845
Troubleshooting Configuration Manager Database Replication 845
Data Types 847
DRS Initialization 848
Additional Tools 852
Server-Based Tools 852
Client-Based Tools 856
The Bottom Line 860

Appendix • The Bottom Line 861
Chapter 2: Planning a Configuration Manager Infrastructure 861
Chapter 3: Migrating to Configuration Manager 2012 862
Chapter 4: Installation and Site Role Configuration 865
Chapter 5: Cloud Integration 867
Chapter 6: Client Installation 867
Chapter 7: Client Health 869
Chapter 8: Application Deployment 869
Chapter 9: Software Updates 870
Chapter 10: Operating System Deployment 871
Chapter 11: Inventory and Software Metering 872
Chapter 12: Asset Intelligence 873
Chapter 13: Reporting 874
Chapter 14: Compliance Settings 875
Chapter 15: System Center Endpoint Protection 877
Chapter 16: Mobile Device Management 878
Chapter 17: Role-Based Administration 879
Chapter 18: Disaster Recovery 880
Chapter 19: Troubleshooting 881

Index *883*

Introduction

The Microsoft System Center product group has completed one of the most successful management products of all time. This group of people works very hard to ensure the product meets the highest standards and is always looking for feedback about it.

This book is written by a group of individuals who have endured the growing pains of this product, some even from day one, and who have even helped Microsoft improve Configuration Manager with countless hours of real-world use and testing.

Welcome to *Mastering System Center 2012 R2 Configuration Manager*. We have provided information for you to become a master in the System Center 2012 R2 Configuration Manager product; you will get the knowledge that is needed to unlock ConfigMgr 2012 R2 to its full potential.

The Mastering Series

The Mastering series from Sybex provides outstanding instruction for readers with intermediate and advanced skills in the form of top-notch training and development for those already working in their field and provides clear, serious education for those aspiring to become pros. Every Mastering book includes the following:

- Real-world scenarios, ranging from case studies to interviews that show how the tool, technique, or knowledge presented is applied in actual practice
- Skill-based instruction, with chapters organized around real tasks rather than abstract concepts or subjects
- Self-review questions, so you can be certain you're equipped to do the job right

What This Book Covers

Mastering System Center 2012 R2 Configuration Manager covers Microsoft's System Center 2012 R2 Configuration Manager. We detail the changes to Configuration Manager since 2007.

These new features include, but are not limited to, the following:

- A completely new mechanism for content distribution — focusing on the needs of the user while retaining the ability to distribute to systems as well
- A user self-service catalog for content deployment
- Updates to software update management and operating system deployment

- The ability to manage mobile devices, including Windows Phone, iPhones, iPads, Android, and more
- A robust alerting mechanism
- A redesigned infrastructure to increase scale and reduce complexity
- The ability to manage profiles with Compliance Settings
- Integration with the cloud, using Windows Azure and Intune

What You Need to Get the Most Out of This Book

To be able to follow the step-by-step instructions in this book, it is recommended that you have a minimum of Windows Server 2008 R2 x64 and SQL Server 2008 R2 with all the applicable updates installed; read more on this subject in Chapter 2. Also, make sure you have the media for Configuration Manager 2012 R2, because we will go through installing this software in the first few chapters. Your computer also needs an Internet connection so you can download updates in various parts of the installation process. Evaluation versions of any of this software are fine for our purposes.

How We Structured This Book

To help you understand the features of Configuration Manager, we have structured this book to match the names of features as they are listed in the Configuration Manager administrative console wherever possible, with a few exceptions.

Chapter 1, "Overview of Service Management," covers general management concepts, such as ITIL and MOF, and how System Center 2012 R2 Configuration Manager supports those concepts.

Chapter 2, "Planning a Configuration Manager Infrastructure," covers site roles, how they are leveraged, and their application in your enterprise.

Chapter 3, "Migrating to Configuration Manager 2012," covers the process of moving from ConfigMgr 2007 to ConfigMgr 2012 and from one ConfigMgr 2012 installation to another ConfigMgr 2012 installation. Discussions include planning the migration, using the new migration tool, and more.

Chapter 4, "Installation and Site Role Configuration," covers the details of site role installation, configuration, and troubleshooting.

Chapter 5, "Cloud Integration," covers the integration of ConfigMgr 2012 R2 with Windows Azure and Intune to manage your devices or BYOD.

Chapter 6, "Client Installation," covers client installation aspects in relation to Configuration Manager 2012, such as the various installation methods found within Configuration Manager 2012.

Chapter 7, "Client Health," covers the new mechanism ConfigMgr 2012 uses to help ensure clients remain healthy.

Chapter 8, "Application Deployment," provides a comprehensive look at planning, configuring, and using the new application deployment model in ConfigMgr 2012, including elements such as deployments, deployment types, dependencies, rules, and relationships.

Chapter 9, "Software Updates," gives you a step-by-step guide of this completely redesigned feature that is now based on Windows Server Update Services.

Chapter 10, "Operating System Deployment," gives you an in-depth look at how Configuration Manager 2012 allows an administrator to deploy a single operating system to multiple types of machines.

Chapter 11, "Inventory and Software Metering," focuses on the heart of Configuration Management Server 2012, one of the core features that most other features tie into.

Chapter 12, "Asset Intelligence," covers the mechanism ConfigMgr 2012 uses for tracking assets, including hardware, software, and licensing.

Chapter 13, "Reporting," discusses probably the most used aspect of Configuration Manager by users outside the IT department. It gives other users the ability to report on various parts of Configuration Manager.

Chapter 14, "Compliance Settings," offers an in-depth look at setting up a predefined level of standards for all your devices and how Configuration Manager 2012 will ensure your clients are maintained at that standard.

Chapter 15, "System Center Endpoint Protection," details the use of ConfigMgr to manage malware protection throughout the computing environment.

Chapter 16, "Mobile Device Management," gives you an inside look at mobile devices and how Configuration Manager 2012 can manage these types of devices.

Chapter 17, "Role-Based Administration," covers the new approach to security in ConfigMgr 2012. Role-based security is used to assign the access needed for specific job functions.

Chapter 18, "Disaster Recovery," provides the information necessary to protect your Configuration Manager databases by backing them up properly so that you can use those backups to recover from a disaster if it strikes.

Chapter 19, "Troubleshooting," shows how to ensure your Configuration Manager 2012 environment stays healthy and gives you a baseline of where and what to look for if problems arise.

Errata

We have done our best to make sure that the content in this book is as accurate as possible at the time it was written. If you discover any mistakes that we have missed in the editing process, please let us know at `http://sybex.custhelp.com` so we can address them in future versions of this book.



Chapter 1

Overview of Service Management

System Center 2012 R2 Configuration Manager (SCCM), like the previous versions of the product, plays an important role in service management in the information technology (IT) world. As IT professionals, we are not responsible for every task required to accomplish a key business activity in our environments. However, we are an important piece of the IT service management process. IT is in the business of providing key capabilities, called *services*, to enable the business functions to achieve the goals of the business. This is one of the many reasons to leverage the Microsoft Operations Framework (MOF) or the IT Infrastructure Library (ITIL) to optimize your IT investment and realize business value.

The idea behind MOF and ITIL is to align IT with the business goals by breaking down silos between IT departments with the ultimate goal of service excellence. Numerous groups fall under the IT department tag, but we often see many of them acting as separate departments rather than as one cohesive unit. Desktop support, application developers, server support, storage administrators, and so on are all members of IT, but they are not always as unified as they should be when delivering quality IT services. Often they lack clarity about who owns each component in the ultimate delivery of the IT service.

System Center 2012 R2 Configuration Manager was built with MOF and ITIL in mind, so we will start the book by describing these two frameworks and how they are central to the mission of the Microsoft System Center family of products. System Center Configuration Manager, or ConfigMgr, is much more than just a mechanism to deploy software. In this chapter, you will learn how we define IT service management and how MOF and ITIL can be the foundation for defining service management in your organization's services throughout the entire lifecycle of those services. You will also learn about how all of the Microsoft System Center products map to service management and the new features of ConfigMgr.

Understanding IT Service Management

The IT Infrastructure Library and the Microsoft Operations Framework were introduced as a way to deliver consistent IT service management (ITSM). Some of the key objectives of ITSM are as follows:

- To align IT services with current and future needs of the business and its customers
- To improve the quality of IT services delivered
- To reduce the long-term cost of service provisioning

Think of ITSM as a conduit between the business and the technology that helps run the business. Without a proper conduit in place, one cannot function properly without the other. ITSM is about people, process, and technology, *not* solely about software products. Although the goals of MOF and ITIL are primarily the same, there are many differences in their implementation. We will discuss both approaches. For a direct cross reference between the two frameworks, download Microsoft's white paper ("Cross-Reference ITIL® V3 and MOF 4.0") for free at `http://www.best-management-practice.com/gempdf/cross_ref_itilv3_mof4.pdf`.

Exploring the IT Infrastructure Library

ITIL at its core is a collection of IT industry best practices organized around a model called the Service Lifecycle. ITIL was first authored in the 1980s and 1990s under the direction of the Central Computer and Telecommunications Agency (CCTA), which became the Office of Government Commerce (OGC) of the United Kingdom. In its current version, ITIL V3 is owned and administered by a joint venture between the UK's Cabinet Office and Capita, plc. If you're interested in these IT best practices, as well as how the Microsoft System Center family of products fits into these processes, you will find the rest of this chapter very interesting. There is also a great blog on the subject by Andrew Fryer (`http://blogs.technet.com/b/andrew/archive/2012/01/09/itil-and-system-center-2012.aspx`). Our focus is on the processes and functions central to ConfigMgr's solutions.

If you start researching ITIL, you will find that it is a series of books describing an approach to IT service management. If you really want to get cozy with ITIL, be prepared to spend a lot of time reading. The Service Lifecycle consists of five components, each a volume of the ITIL V3 core books:

- *ITIL Service Strategy*
- *ITIL Service Design*
- *ITIL Service Transition*
- *ITIL Service Operation*
- *ITIL Continual Service Improvement*

There is much more to ITIL than just the books, however. ITIL as a whole includes the books, certification-accredited trainers and examination institutes, ITIL consultants, white papers, and ITIL-based training and user groups (like itSMF, the IT Service Management Forum). The scope of ITIL is far beyond what will be described in this chapter, so what you will want to take away is where the features provided by ConfigMgr intersect with ITIL. Table 1.1 maps ITIL V3 against Microsoft's System Center 2012 product line. Note the designations of SCCM fall into two phases: Service Transition and Service Operation. More specifically, the processes of Change Management, Service Asset, Configuration Management, and Release and Deployment Management fall under Service Transition, and the functions of IT Operations Management and Application Management fall under Service Operation.

The interrelations of all of these processes and functions will become more and more evident the more deeply we discuss the features of ConfigMgr and how it supports these processes and functions within ITIL.

Table 1.1: ITIL V3 mapped to Microsoft System Center product line

ITILV3 Phase	ITILV3 Process	Level	SC 2012 1st Phase	SC 2012 2nd Phase
Service Strategy	Strategy Generation	×		
	Financial Management	×		
	Service Portfolio Management	✓	SCSM	
	Demand Management	!		SCOM
Service Design	Service Catalog Management	×	SCSM	
	Service Level Management	×	SCSM	SCOM
	Capacity Management	×	SCOM	SCVMM
	Availability Management	×	SCOM	SCVMM
	IT Service Continuity Management	×	SCOM	SCDPM
	Information Security Management	×	SCCM	SCSM
	Supplier Management	!	SCSM + Third Party	
Service Transition	Transition Planning and Support	×		
	Change Management	✓	SCSM	SCCM
	Service Asset and Configuration Management	✓	SCSM	SCCM
	Release and Deployment Management	✓	SCSM	SCCM
	Service Validation and Testing	✓	SCOM	SCVMM
	Evaluation	✓	SCOM	SCVMM
	Knowledge Management	✓	SCSM	SCOM
Service Operation	Event Management	✓	SCOM	SCOM
	Incident Management	✓	SCSM	
	Request Fulfillment	✓	SCSM	SCOM

TABLE 1.1: ITIL V3 mapped to Microsoft System Center product line *(CONTINUED)*

ITILV3 PHASE	ITILV3 PROCESS	LEVEL	SC 2012 1ST PHASE	SC 2012 2ND PHASE
	Problem Management	✓	SCSM	SCSM
	Access Management	!		
	Service Desk	✓	SCSM	SCOM
	Technical Management	!		SCCM
	IT Operations Management	✓	SCOM	SCCM
	Application Management	✓	SCOM	SCOM
Continual Service Improvement	7 -Step Improvement Process	!		SCOM
	Service Reporting	✓	SCOM	SCVMM
	Service Measurement	✓	SCOM	SCVMM

✓ = *Requires little or no customization*

! = *Requires customizations*

Credit: Cleber Marques, Microsoft Consultant, Brazil

SERVICE STRATEGY

The Service Strategy phase is at the center of service management because everything that you execute upon using processes, people, and technology is aligned to employ your service strategy. The service strategy is born out of business strategies to develop markets and manage risks and costs. The strategy is leveraged in every other phase of ITIL to enable the capabilities required by the business. The processes associated with this phase are Strategy Generation, Financial Management, Service Portfolio Management, and Demand Management.

SERVICE DESIGN

The Service Design phase takes you through the process of transforming your service strategy into a portfolio of services considered to be strategic assets of the business. The processes involved in this phase are Service Catalog Management, Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management, and Supplier Management. As you may have deduced already, these activities are focused on not merely the features of the service but also the quality of the service to ensure the businesses requirements are met.

Service Transition

Each IT service changes over time, based on many factors related to the needs of the business (for example, regulatory compliance, new feature requests, software updates, and the like). This phase delivers new and changed services based on specifications of the service design, in accordance with the service strategy. This important step represents the emergence of the IT service, and Systems Center Configuration Manager plays a central role in this phase. The processes involved in this phase are Transition Planning and Support, Change Management, Service Asset and Configuration Management, Release and Deployment Management, Service Validation and Testing, Evaluation, and Knowledge Management.

Service Operation

The Service Operation phase focuses on effective and efficient delivery of the service day to day. The objectives laid out in your strategy are realized only through the operation of the service, which makes this step critical to implementation of an effective IT service. Again, you find Systems Center Configuration Manager squarely planted in this phase delivering value. The processes involved in this phase are Event Management, Incident Management, Request Fulfillment, Problem Management, and Access Management.

This is the only phase in ITIL that provides guidance on specific IT functions. These functions are Service Desk, Technical Management, IT Operations Management, and Applications Management. These functions are defined not to describe an organization but to map out the processes or activities that must be carried out by an organization.

Continual Service Improvement

The central theme of Service Management is to provide incremental and large-scale improvements to the IT services delivered to the business. This phase surrounds all the other ITIL phases and provides guidance on connecting improvement project outcomes to service strategy, design, and transition. The processes involved in this phase are 7-Step Improvement Process, Service Reporting, and Service Measurement.

Select ITIL Functions and Processes

The scope of ITIL expands far beyond the functions and processes supported by ConfigMgr, so in this section we will explore the particular ITIL functions and processes that do correspond to ConfigMgr.

Service Desk

We will look at the service desk, because all incident reporting and service requests are routed through the service desk. It is the function that ties the service providers with the users, keeping users informed of service events and actions that may impact their day-to-day activities. The service desk becomes a single point of contact for customers and users to interact with the IT department. This approach helps expedite the call process by managing it in a timely and satisfactory way. There are features in ConfigMgr, such as out-of-band management and remote control, that can greatly enhance the user experience. Note that these service requests and incidents are also transformed into changes and deployments that will be implemented using ConfigMgr.

IT Operations Management

The IT Operations Management function is responsible for crisp execution of the day-to-day activities needed for keeping the IT services running smoothly, reliably, and cost effectively. Activities like console management and job scheduling are firmly rooted in this function. Thus, ConfigMgr activities such as software updates, security patch management, end-point protection, and several other capabilities are a central part of keeping IT infrastructure running efficiently and effectively.

Applications Management

The Applications Management function is focused on the Application Lifecycle, which is closely aligned to the Service Lifecycle but differs significantly. This function is responsible for the design, testing, and improvement of applications. Needless to say, ConfigMgr can enhance the ability to package, deploy, and patch these applications. There is even the option of virtualizing these applications across the enterprise.

Technical Management

The Technical Management function typically comprises multiple departments organized by specific technical skill sets (servers, network, database, telecommunications, and so on). Often the care and feeding of the ConfigMgr platform are assigned to one or more departments in this function.

Incident Management

Incident management is the mechanism by which the service desk records, updates, and tracks the enterprise "fires." The Incident Management process is mainly concerned with restoring normal service operations as soon as possible. This will help minimize any adverse effects on business operations and will ensure high levels of service quality and availability. Service-level agreements (SLAs) determine what a normal service operation is. Information is collected about the incident to allow changes or enhancements in the environment to prevent future incidents. The ability to determine the scope of impact of an incident is often tied to knowing how many service assets are deployed across the enterprise that could be affected by the particular incident. ConfigMgr has the ability to provide counts of qualified assets across the entire enterprise.

Problem Management

The Problem Management process is mainly concerned with minimizing the impact of problems, which are often the root cause of incidents. The goal is to reduce incident resolution times by providing insights for known errors and removing the underlying causes. This strategy improves IT service quality by helping the service desk resolve incidents promptly at the time of logging. If an incident can be resolved at the time of logging, business impact is reduced, business efficiency is improved, and IT efficiency is improved.

The Problem Management process should not be considered a reactive-only approach, however. When dealing with incident management, problem control, or error control, it is very reactive. The Problem Management process can be viewed as proactive when you consider how it is used for problem prevention.

Problem investigation and diagnosis come into play when known errors are created. During this investigation and diagnosis period, insightful details of the known errors are captured and communicated until a fix for the problem is found. ConfigMgr contributes proactively to this process in its client health and monitoring and compliance and settings management capabilities.

Service Asset and Configuration Management

The Service Asset and Configuration Management (SACM) process is responsible for keeping an accurate and up-to-date model of the entire IT infrastructure. It uses this information to help support a number of areas by doing the following:

- Allowing for assessment of service impact for Incident, Change, or Problem Management processes
- Allowing financial information to be gathered to help determine lease, rental, maintenance, and support costs for IT infrastructure components
- Supplying information about component performance and reliability to support capacity and availability management
- Improving security by identifying the location and details of assets, making it difficult for unauthorized changes to be carried out undetected
- Helping with legal obligations by identifying the location of unauthorized software, determined by enabling authenticity checks on software and making sure current, correct versions of the software are being used

SACM also correlates information to identify relationships between configuration items. These relationships provide insights into dependencies for changes and can help in the resolution of incidents and problems. Many of the ITIL processes rely on accurate service asset information for effective and efficient results. This becomes critical in the realm of service compliance to policy, such as Security policy and others. Many organizations suffer from incidents (including service outages and performance issues) as a result of IT service operations. Many of these operational issues stem from misconfiguration. There is substantial benefit from implementing ConfigMgr to avoid misconfiguration and optimize your IT capabilities and resources.

Change Management

The Change Management process ensures that standard methods are used when implementing change and for developing and documenting reusable processes. Implementing a change-management system can reduce the possibility that a change in the environment could cause a failure, thus resulting in an incident or rework.

The IT infrastructure is constantly changing. Patches, service packs, updates, firmware, drivers, and so on are released on an almost daily basis. Also, evolving business requirements require thoughtful change. Having a repeatable process in place to accomplish these changes while minimizing risk and cost to the business is vital. Enhancing this process using an automated software distribution and policy-management tool like ConfigMgr can ensure that changes to software, policies, and settings are consistently delivered across the entire enterprise.

Release and Deployment Management

Changes in the environment and the business marketplace often result in the need for new iterations of software, hardware, documentation, and the like. The Release and Deployment Management process works closely with Change Management and SACM to produce a secure and managed rollout of the new package of service assets or version of the service itself. The resulting live service is tested to ensure that it meets the objectives defined in the service strategy and delivers the capabilities defined in the service design.

Many of the features of ConfigMgr are embodied in this process. Whether it is software update management, application delivery, virtual desktop management, operating system deployment, or endpoint protection, System Center Configuration Manager securely delivers service assets that can provide immediate value across your organization. If your IT organization is affected by BYOD (bring your own device) scenarios that extend the need for services beyond IT-owned assets, ConfigMgr can partner with Windows Intune to deliver value across those devices as well.

Service Level Management

The Service Level Management (SLM) process is responsible for creating service-level agreements (SLA) between IT and the business. SLAs play an important role in SLM. They help set expectations for IT by determining the customer's service-level requirements, and they help customers by providing a measurable definition of good service. Both sides can agree on timelines for deliverables for everything from service upgrades to updates to incident resolution. SLAs also provide a clear understanding of what value customers are receiving from IT. ConfigMgr can help in both delivery and measurement of some service levels, particularly related to software updates and client management.

Financial Management

The Financial Management process is responsible for determining the costs of IT services as well as calculating the return on IT service investments. Prudent use of IT assets drives efficiencies that return value to the business. ConfigMgr can help optimize timely deployment of IT assets across the entire enterprise, resulting in greater returns on the IT investments.

Capacity Management

The Capacity Management process involves determining the required service delivery, the current service delivery, and the IT infrastructure and ensuring that all current and future capacity and performance requirements from the business are met. ConfigMgr can assist in delivering insights into usage and inventory of key service assets to increase the agility of the IT organization in delivering timely service improvements.

IT Service Continuity Management

The IT Service Continuity Management process ensures that an organization can continue to function with predetermined and agreed-on levels of IT services to support the minimum business requirements following a catastrophic interruption to the IT service. The idea behind this process is that the organization will always have a base level of required IT services available to perform critical business functions.

Each IT service is examined to determine the minimum level it can function at to meet the business requirements. A plan is then put in place to guarantee that this level of service can be reached at all times under any circumstances. ConfigMgr can greatly enhance an organization's ability to recover these services through repeatable automation to rebuild systems, clients, and applications across the enterprise.

Exploring the Microsoft Operations Framework

The Microsoft Operations Framework was originally developed by Microsoft and a group of partners to expand on the best practices developed by ITIL. It has since been rewritten for its current version (V4.0) to follow a service lifecycle format using three sequential phases (Plan, Deliver, Operate) with one layer underlying all phases (Manage), which compose the four major components of the framework. These components are supported by specific guidance in the form of service management functions (SMF). MOF includes a plethora of resources that are available to help you achieve mission-critical system reliability, manageability, supportability, and availability with Microsoft products and technologies. These free resources, called Solutions Accelerators, consist of a series of phase overviews and SMF guides. There are also documents detailing the management reviews (milestones defined in the lifecycle), companion guides, job aids, action plans, and more. They describe the activities that need to occur for successful IT service management—from the assessment that launches a new or improved service, through the process of optimizing an existing service, all the way to the retirement of an outdated service.

The guidance is written for a number of audiences: corporate information officers (CIOs), IT managers, and IT professionals:

- Overview guides are directed toward CIOs who need to see the big picture.
- Overview and workflow information in function-specific guides is geared toward IT managers who need to understand the IT service strategies.
- Activities in function-specific guides are meant for the IT professionals who implement MOF in their work.

If you are interested in the detailed MOF guidance, it is available on Microsoft TechNet at `www.microsoft.com/mof`.

Table 1.2 illustrates each of the MOF components and its associated SMFs. To the right of each SMF a key capability of System Center Configuration Manager is noted that relates to that SMF.

Table 1.2: MOF/SCCM breakdown

Component	SMF	SCCM
Plan phase	Business/IT Alignment	Reporting
	Reliability	
	Policy	
	Financial Management	Reporting

TABLE 1.2: MOF/SCCM breakdown *(CONTINUED)*

COMPONENT	SMF	SCCM
Deliver phase	Envision	
	Project Planning	
	Build	
	Stabilize	
	Deploy	Deploy
Operate phase	Operations	Deploy
	Service Monitoring and Control	Monitor
	Customer Service	Remote
	Problem Management	Health
Manage layer	Change and Configuration Management	Deploy
	Governance, Risk, and Compliance	Compliance settings
	Team	

The goal of the Plan phase is to get IT and the business together to begin aligning service plans to the needs of the business. The desired outcome is a well-planned service portfolio that delivers reliable capabilities to the business within compliance and cost guidelines. Ideally, IT will be in a position to quickly adapt to changing business needs as well. The reports regarding usage and inventory of service assets produced in ConfigMgr will assist in the Business/IT Alignment and Financial Management SMFs.

The Deliver phase is an adaptation and integration of what used to be called the Microsoft Solutions Framework (MSF). This phase is where the strategic plans of the previous phase are realized and delivered as production services into the next phase. ConfigMgr greatly enhances an enterprise's ability to deploy services across the enterprise and beyond.

The Operate phase deals directly with the health of the service. It prescribes how to proactively ensure the service is available, reliable, and cost effective through monitoring and execution of routine maintenance for problem resolution. There is also a need to quickly recover from service incidents when they occur. ConfigMgr can significantly reduce costs and increase reliability of maintenance like security patching and endpoint protection. It can also provide alerts when systems are out of compliance with required settings and policy.

Select MOF Service Management Functions

Service management functions are the underlying process and activities within each Microsoft Operations Framework phase and support the mission of service for that phase. These SMFs are the core of the MOF process model, although all of the SMFs are cross functional.

Business IT Alignment

This is where the IT service strategy is born by close cooperation of IT and the business. Knowledge of service demand and usage is required to successfully deliver this SMF. ConfigMgr can help provide insights in the usage and current capacity investigations, particularly through queries.

Financial Management

Similar to the process of the same name in ITIL, there is an essential need to account for the cost of delivering required IT services. Measuring service assets such as devices and software licenses is available in ConfigMgr.

Deploy

As the final step in the Deliver phase, Deploy put the emphasis on successful transition of tested services into the production environment. This means that the operations and support teams are fully prepared to manage the service. It also means that as you deploy it across the enterprise, ConfigMgr can ensure that it is done consistently and identify anywhere that the deployment might have failed.

Operations

Operations is all about running the service efficiently and effectively to meet established service levels. Automation of routine maintenance as is provided in ConfigMgr greatly improves your ability to deploy changes cheaply with repeatable success and reliability when done properly through the settings management feature.

Service Monitoring and Control

Watching the service and measuring its availability are critical to meeting service levels and responding to service incidents in a timely manner. This SMF minimizes outages by ensuring that service assets are monitored and controlled. ConfigMgr has features like Network Access Protection and Setting Management that help ensure key infrastructure meets required standards and policy.

Customer Service

This SMF focuses on the customer and the end users who deliver value to the business by use of the service. The ability to use ConfigMgr to better service these users remotely and use out-of-band management can tremendously improve the users' support experience.

Problem Management

Almost identical to the ITIL process of the same name, this SMF tackles reducing the numbers of incidents through problem resolution and proactively avoiding incidents by identifying and resolving problems. The ConfigMgr client health and monitoring feature really exemplifies a tool to engage successfully in the effort of troubleshooting or monitoring potential problems.

Governance, Risk, and Compliance

This SMF focuses on growing the organization while managing its risk. ConfigMgr enables real policy compliance that can be consistently applied across the entire enterprise.

Change and Configuration Management

The focus of this SMF is to limit service disruptions by managing planned changes and consistently configuring service assets properly. Unplanned changes are minimized and tracked as a way of normalizing change in the enterprise to align with required service levels. ConfigMgr takes on a number of complex challenges to deliver solutions to change in an enterprise environment. Features such as collections can identify and organize specific sets of service assets for remediation like Mobile Device Management to distribute software and settings to the plethora of mobile devices proliferating throughout the enterprise.

Operations Management Reviews

Several milestones plotted along each MOF phase in the lifecycle bring together the required outcomes and functions to ensure readiness for the impending phase. Based on the requirements of this discussion, we do not need to delve into these reviews, but we did want to make you aware that they form a critical piece of MOF.

Overview of System Center Configuration Manager

So far you have read about the IT Infrastructure Library and Microsoft Operations Framework and now have a better understanding of the IT process and its phases. Now let's look at System Center 2012 R2 Configuration Manager, explore the new features of the product, and examine how the product has developed into an enterprise management tool that provides a total solution for Windows client and server management. ConfigMgr includes the ability to acquire hardware and software inventory in order to identify the assets of the enterprise. It provides a wide variety of features that include delivery of new software packages, virtual applications, software updates, and operating systems, and it also ensures the systems are protected with the latest antivirus definitions. All of these features are available through a single centralized console. ConfigMgr provides IT administrators with the capability to stay in control of the environment and help configure, manage, and secure the clients and applications.

Configuration Manager Features

Before you can begin planning to deploy Configuration Manager on your network, you need at least a basic understanding of the features that Configuration Manager provides. For veteran SMS 2003 and Configuration Manager 2007 administrators, these features will not be very different from what you are already familiar with. For those that are new to the product, the original product name was called System Management Server, and it started with version 1.0. However, you will find several new features added to Configuration Manager 2012, several features that were feature packs or add-ins in SMS 2003, and others that have been improved from Configuration Manager 2007. Configuration Manager 2012 no longer takes advantage of the Microsoft Management Console (MMC) technology for the administrator console; instead, each administrator console has its own stand-alone application, as shown in Figure 1.1.

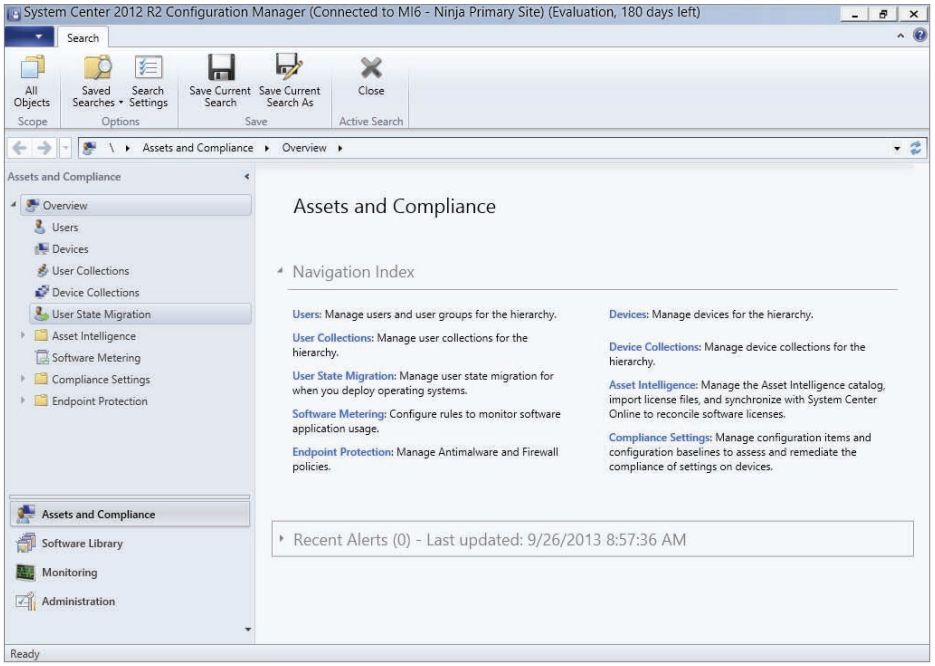


FIGURE 1.1 Microsoft Configuration Manager 2012 console

The major features include the following:

Inventory Configuration Manager offers you the ability to inventory the hardware and software of its client computers. Hardware inventory can gather information from your systems such as processor information, the computer manufacturer, and the amount of installed memory. Software inventory can gather lists of file types and their versions installed on your computers, with EXE files being the default. Combine this with extensive information in the Asset Intelligence (AI) knowledge base, and you can use Configuration Manager to really get a handle on what kinds of hardware and software are being used in your environment.

Inventory is the backbone of Configuration Manager; you can run Configuration Manager without enabling inventory, but you really wouldn't be able to do much, since so many other features, such as software updates, require inventory. Inventory is just about the same as it was in SMS 2003 and Configuration Manager 2007. Inventory is a very important piece of the MOF quadrant. Operations management is easy to maintain with a proper inventory of the IT environment; without one it's very hard to maintain detailed information about the infrastructure and the current assets. We will go into more detail about this feature in Chapter 11, "Inventory and Software Metering."

Queries Queries allow you to gather information from the Configuration Manager database through the WBEM query language (WQL). This allows you to answer questions quickly or make mini-reports that might not be used often enough to be imported into the reporting interface. You can export these reports from the Configuration Manager console into different file formats and then email them for others to use in programs such as Microsoft Excel.

Queries are primarily used to make groups of Configuration Manager resources, called *collections*, that are used by other Configuration Manager features. These queries are a good way to identify resources based on WQL. Parameters entered in the queries GUI inside Configuration Manager can simplify the reuse of code within a collection. As you can see, queries are a very important piece of the Capacity Management process in the Service Design phase in ITIL and the Plan phase of MOF.

Collections Collections can be the answers or results to a question that involves specifying various resources, such as, "Which resources are running Windows XP Professional Service Pack 2 with more than 2 GB of RAM, with more than 1 GB of free disk space, and with a certain BIOS version?" Collections allow you to organize Configuration Manager resources into logical groups, based on a query. A collection can target Configuration Manager tasks to the resources that you specify. You can make collections based on queries, allowing them to be updated dynamically based on a configurable schedule or by directly assigning resources. Collections can consist of computers, users, user groups, or any discovered resources in the Configuration Manager database. Collections, as a fundamental feature, have not changed much since SMS 2003 or Configuration Manager 2007, but they are now the necessary building blocks used to enable other features such as maintenance windows and collection variables. Collections are a good way to analyze and organize resources; they can also depend on the Capacity Management process in Service Design phase of ITIL and the Plan phase of MOF.

Application Management This feature allows Configuration Manager to distribute just about anything to its client computers. This is probably the most-used feature of all the previous versions of Configuration Manager, and it's probably the most dangerous if not used carefully. It is likely that just about all SMS admins have accidentally deployed a piece of software that they shouldn't have (if you haven't, then keep up the great work!). This isn't a fault of this feature but something that can happen if you don't test, test, test, and then test again. Anything you plan on deploying to client computers must be carefully managed, and you must pay close attention to the details of what you are doing.



Real World Scenario

Using AdminStudio Configuration Manager Edition

It is important to note that Configuration Manager is just the method of distribution; it doesn't have any built-in capability to package software before it is distributed. You will have to use another piece of software to do that yourself. Microsoft has licensed AdminStudio Configuration Manager Edition to give administrators a reliable and repeatable process to assist in creating Windows Installer packages. This, of course, is where the testing comes in. This feature has had numerous improvements since SMS 2003, such as the deployment of not only physical applications but also virtual applications, as well as improvements since Configuration Manager 2007, but overall it works basically the same as it did before. Application Management is part of Systems Management in ITIL and the Changing quadrant of the MOF.

Software Updates This feature of Configuration Manager has to be one of our favorites. Using this feature, you can manage the daunting task of deploying updates to Microsoft applications and operating systems Not only does this apply to Microsoft security patches and

updates, but having this flexible and extensible environment has allowed partners (such as HP, Dell, IBM, Citrix, and others) to create custom catalogs to update server and desktop BIOS, firmware, and drivers as well as to create internal catalogs. This enables customers to create their own line-of-business application update catalogs and update them through the same streamlined process as Microsoft uses for patch management.

Deploying updates requires a Windows Server Update Services (WSUS) server. Configuration Manager leverages WSUS with its own functionality and provides a higher level of granularity than is available with WSUS alone. Software updates are an important phase in the Incident Management process and IT Operations Management function of ITIL and the Operate Phase in MOF. We will cover software updates in more detail in Chapter 9, "Software Updates."

Software Metering Software metering, also covered in Chapter 9, allows you to collect information on software usage to assist in managing software purchases and licensing. Using software metering, you can do the following:

- Report on the software that is being used in your environment and on which users are running the software
- Report on the number of concurrent users of a software application
- Report on software license requirements
- Find unnecessary software installs
- Find software that is installed but isn't being used

The new twist to software metering is that the metering rules are autopopulated, or created, but disabled by default, based on the software inventory. This allows you to rapidly meter applications and gain insights into usage. SMS 2003 had metering, but it was cumbersome to figure out the appropriate rule setup. This now is a thing of the past. Software metering is part of the Service Measurement process in ITIL and Change and Configuration SMF in MOF. Based on the utilization of software, you can measure when applications are properly used in the environment for better inventory of the current assets.

Operating System Deployment This feature was originally released as a feature pack for SMS 2003. It was workable but was a minimalist approach that was sometimes difficult to implement and troubleshoot. Configuration Manager not only has this feature fully integrated into the product, but it has become a feature-rich, process-driven way to deploy servers and workstations. It leverages other new technology specifically designed by Microsoft to deploy operating systems to computers with multiple options.

Originally this feature supported the deployment of desktops only, but it now supports deploying servers. With the addition of the task sequencer and driver catalog, you can deploy to bare-metal computers or to ones that already have an operating system installed, as well as deploy software to these computers after they have been configured. This allows you to minimize the number of images for different hardware, and it gives you more granular configuration options. Operating system deployment (OSD) is also part of the Changing quadrant of the ITIL and MOF and an important piece of systems management. We will discuss this robust feature in more detail in Chapter 10, "Operating System Deployment."

Remote Control This feature allows computer support staff to remotely troubleshoot problems with users' computers just like they are sitting in front of the computer. This feature is still integrated with Remote Assistance and Remote Desktop, and it works pretty much the same as it did in the previous version.

The ability to support the desktops via remote control is a beneficial part of the Service Continuity Management function for ITIL and MOF.

Settings Management This feature is designed to address configuration drift within the enterprise. Enterprise administrators (for workstations and servers) as well as security teams need a tool that enables them to set configuration baselines (based on SOX, HIPPA, GLBA, or other compliancy regulations), deploy machines to an environment meeting these baselines (for example, with the local guest account disabled, Windows Integrated Security for SQL Server enabled, and so on), and then detect when these changes occur. Microsoft delivers configuration packs that jump-start an organization in the compliancy areas mentioned and allow you to set up a baseline of standards for your workstations and servers and audit your environment against that baseline.

You can configure your own baselines from scratch, or you can use best practices from Microsoft and their partners in the form of Configuration Manager Configuration Packs, which can be modified if needed. The ability to configure, monitor, and remediate the systems based on specific needs is key to IT Operations Management and Operations on ITIL and MOF, respectively. This feature will be covered in Chapter 14, "Compliance Settings."

Mobile Device Management This feature allows you to manage mobile devices such as Windows Mobile Pocket PCs and smartphones. Inventory, file collection, software distribution, and device configuration are all options with this feature. This was an add-on feature in SMS 2003 and is now fully integrated into Configuration Manager. New environments are bringing mobile devices to each environment. There is a need to support mobile devices to ensure that IT is running on the same track as the consumer. This feature will be discussed in Chapter 16, "Mobile Device Management."

Network Access Protection This is a new feature in Configuration Manager. It leverages technology built into Windows Vista and Windows Server 2008 that allows you to protect your network from potential threats by not allowing computers to access your network that do not meet certain system health requirements such as having updated antivirus definitions or security patches installed. With this feature you can also enforce certain network protocols. The ability to secure the environment is one of the tasks on the Supporting and Operating quadrants on ITIL and MOF. Chapter 19, "Troubleshooting," covers this feature.

Wake on LAN This feature, added to software distribution, was available in SMS 2003 only by purchasing third-party software. It allows you to leverage technology built into computer hardware to wake up computers that have been turned off so they can run assigned deployments. Chapter 8, "Application Deployment," shows how to enable it. This option brings more power to the tasks of the Operating and Supporting quadrants for the ITIL and MOF.

Reporting This feature is great for reviewing the status of the environment, for showing return on investment, and for matching licensing with what is actually installed. It grants visibility into the enterprise with the integration of Asset Intelligence (covered in Chapter 12, "Asset Intelligence"). This allows you to gain an understanding of licensing (Microsoft and third-party licenses), asset age, Client Access License (CAL) utilization, product families/categories, and much more insightful data. With this feature you can create

web-based reports, via Configuration Manager or through SQL Reporting Services, that can show all the data that has been collected by the various other Configuration Manager features, such as software update deployment success or a list of computers of a certain manufacturer.

You can also group together commonly viewed reports into dashboards for easy viewing with just one click. Numerous reports are already created out of the box, and you can create your own custom reports with a little knowledge of SQL queries. In ConfigMgr 2012 the only report option is based on Reporting Services. This is the most beneficial piece of service management for ITIL and MOF: being able to report everything that is going on with the IT resources makes the job of auditing and reporting a simple one. Reporting is discussed in several chapters and is covered fully in Chapter 13, "Reporting."

Out-of-Band Management A business challenge that has been a struggle for years is the ability for software to communicate directly with hardware. Let's say, for example, that you're supporting a worldwide organization and have a centralized help desk. You have a desktop that is thousands of miles away, and the user has contacted you because of an operating system blue screen. A typical support remediation from years past would be to create a ticket so that a local technician would be able to physically visit the location.

Intel introduced manageability directly into its chip set with the Intel Active Management Technology (AMT) initiative; the direct result was the Intel vPro desktop processor. Intel and Microsoft worked on a strategic management initiative so that software could communicate directly with hardware. Now, when a user contacts the help desk with that same scenario, a help desk administrator can actively engage and potentially resolve an issue without needing to escalate a ticket to another team.

Configuration Manager leverages four key areas to communicate directly to hardware. These areas may be leveraged holistically within an organization's standard operating procedures for in-band and out-of-band management to provide a streamlined resolution process. In-band management is used when the Configuration Manager client agent is functioning, and out-of-band management occurs when software communicates with hardware because no other means may apply. These are the four areas:

Discovery Discovery is an out-of-band management area that provides an administrator with the ability to achieve discovery on demand. This can be performed on a single machine or groups of machines via a Configuration Manager collection. It also allows you to schedule a discovery so that if the software does not respond, the hardware still can provide insight into an asset.

Power Control Power control provides the flexibility to allow both scheduled and on-demand power-on capabilities. From a scheduling perspective, this can potentially improve efficiency and data consistency when used in conjunction with other Configuration Manager features such as software distribution, software update management, or operating system deployment. From an on-demand perspective, this enables administrators to wake up, restart, or shut down a remote machine. One area of efficiency that enterprises are increasingly demanding is power management. Thus, the ability to control hardware and software from a single pane of glass becomes an attractive feature.

Provisioning Provisioning workstations, either as new assets that enter the enterprise or as a means to an end in the remediation process, has become a necessary part of an administrator's role. As the operating system becomes less independent of hardware (that is, the operating system hardware abstraction layer [HAL]), the provisioning process may become more

streamlined. With an integrated solution such as AMT and Configuration Manager, secure, zero-touch setup and provisioning of workstations can be achieved.

Remote Console Remote console for out-of-band management enables administrators to perform advanced techniques such as serial over LAN, IDE redirection, BIOS password bypass, and manual power control. This allows an administrator to remotely mount a bootable troubleshooting image (ISO image), boot into the BIOS to change the boot order, or turn the targeted machine on or off at will.

To that end, when the user contacts the help desk with a nonfunctioning operating system, the help desk administrator can proactively take the appropriate actions. For example, the standard operating procedure might look starkly different from just creating a ticket and dispatching a desktop support technician. It may be that the help desk administrator reboots into the BIOS, leveraging the serial-over-LAN capabilities, and changes the boot order in the BIOS so that the network card is the first in the boot order. From there, a diagnostic tool is mounted with IDE redirection, which shows the administrator that the operating system has some corrupt DLLs. Thus, the administrator can then provision a role-based operating system image to this user to reimage the workstation. A process or help desk ticket that might have been very expensive or time consuming now becomes a streamlined process that results in the user having less downtime and a higher degree of satisfaction with their help desk experience.

Asset Intelligence

Asset Intelligence, which was included within Configuration Manager 2007, now comes with its own node within the Administrator console. This isn't the only new aspect of Asset Intelligence; AI also became part of the Software + Services initiative within Microsoft. The services component of AI is not a fee-based feature but is just another extension of the holistic approach; it includes the following functionality:

- New catalog and license management UI in the Configuration Manager Administrator console
- The ability to customize the local catalog, in other words, create new categories and families
- On-demand or scheduled catalog update synchronization through the Configuration Manager console
- The ability to tap software assets unknown to the catalog and pass them up to the online service for async identification
- The ability to import licensing data from Microsoft and compare it to installed inventory

Asset Inventory is one of the reporting structures used to analyze and ensure that every asset on the system is being used properly and report this to management. This ability is part of change and configuration management for ITIL and MOF; we'll discuss this further in Chapter 12.

Application Virtualization Management

With the newest release of App-V, Configuration Manager 2012 leverages its existing infrastructure and extends its reach to deliver virtual applications:

- It integrates Microsoft App-V 4.6 and App-V 5.0 with ConfigMgr 2012.
- Application Virtualization Management (AVM) allows you to use Configuration Manager to manage and deploy virtual applications, when possible, to make managing virtual applications for the Configuration Manager administrator the same experience as managing standard or physical software.
- AVM has version checking, user-based targeting, and streaming functionality.

Operating System Deployment Enhancements

Although Configuration Manager 2007 was good at deploying operating systems, a couple of improvements were needed in order to compete in the marketplace. The following enhancements now round out the offerings of Configuration Manager in the enterprise:

- With ConfigMgr 2012, an unknown machine can now receive a task sequence to install an operating system.
- There is support for multicasting operating system images to a PXE environment—for well-connected LANs leveraging Windows Server 2008 R2 technologies, on the same distribution point.

SQL Reporting Services Integration

SQL Reporting Services (SRS) is an evolution of reporting just as previous technologies have been. The Microsoft management team has standardized on SRS for reporting within the System Center family of products. The SRS integration within Configuration Manager 2012 enhancements includes the following:

- The new server role Reporting Services point
- The ability to manage, browse, and run SRS Configuration Manager reports from the Configuration Manager console

Centralized Power Management

Saving energy and preserving the environment are important goals for IT professionals and organizations. The ability to control the power-saving settings on workstations is a great achievement for many organizations. Also important are the abilities to monitor the power consumption, create different power plans based on organization need and different operational departments, and check compliance and remediate those workstations that are in noncompliance. It's easy to manage these situations on SQL Reporting Services.

System Center Endpoint Protection

This feature brings the ability to scan and secure system resources from viruses or malware. System Center Endpoint Protection enables businesses to align security and management to improve endpoint protection while greatly reducing operational cost.

Endpoint Protection is built on three pillars: simplify, integrate, and protect.

Simplify Creates a single administrator experience for managing and secure endpoints.

Improves visibility for identifying and remediating potentially vulnerable endpoints.

Integrate Lowers ownership cost by using a single infrastructure for both endpoint management and security.

Deploys effortlessly to hundreds of thousands of endpoints.

Protect Provides highly accurate detection of known and unknown threats.

Actively protects against network-level attacks by managing Windows Firewall configurations.

Summary

Now that you have read about ITIL, MOF 4.0, and a high level overview of System Center 2012 R2 Configuration Manager, it's time to dive into all details related to ConfigMgr 2012 R2. In the next chapter, you will learn about planning a ConfigMgr infrastructure. Make sure to read all subsequent chapters. This book will give you all types of inside information about the product.



Chapter 2

Planning a Configuration Manager Infrastructure

Properly planning a Configuration Manager infrastructure is crucial in utilizing the software to its full potential. This is even more the case with Microsoft System Center 2012 R2 Configuration Manager with its new and improved features.

The first step is to define a project plan with the phases defined in the Microsoft Solution Framework. The Microsoft Solution Framework will guide you to set up a project plan with the following phases:

- Envision: Gather deployment intelligence.
- Plan: Plan and design the Configuration Manager environment.
- Develop: Build the proof-of-concept and the new environment.
- Stabilize: Perform a pilot with multiple key users.
- Deploy: Migrate the users to the new infrastructure.

More information about the Microsoft Solution Framework can be found at the Microsoft TechNet documentation library.

In this chapter, you will learn to

- Plan and design a Central Administration Site
- Plan and design an effective Configuration Manager 2012 infrastructure
- Identify the enhancements to the distribution point site system role
- Prepare your current Configuration Manager 2007 environment for the migration to Configuration Manager 2012

Gathering Deployment Intelligence

When you want to implement a new Configuration Manager 2012 infrastructure in your environment or you want to migrate from Configuration Manager 2007, you need to write a plan of approach. The installation of Configuration Manager 2012 looks like a Next, Next, and Finish installation, but without a solid plan you will not use most of it. It's crucial to describe your current environment and define a goal you want to reach or make a business case for your project. The following sections describe the process in detail.

Three Pillars of Configuration Manager

Configuration Manager 2012 is built on three pillars:

- Empower Users
- Unify Infrastructure
- Simplify Administration

The Empower Users pillar means that Configuration Manager gives the users the ability to be productive from anywhere on whatever device they choose.

The Unify Infrastructure pillar means that Configuration Manager gives the IT department the ability to reduce the cost of the IT management infrastructure. This is done by the simplified Configuration Manager infrastructure and the integration of other technology in Configuration Manager 2012, for instance, by embedding Forefront Endpoint Protection and most of the features of Microsoft System Center Mobile Device Management.

The Simplify Administration pillar means that Configuration Manager will give Configuration Manager administrators a less-complex infrastructure to manage and, with the role-based administration feature, more effectiveness.

Since the positioning of Configuration Manager in the IT environment has changed and has become more important, planning the Configuration Manager environment is essential for an effective implementation of Configuration Manager 2012.

Determining What You Need to Accomplish

Before installing Configuration Manager in your environment, it's wise to define the business case and scope of your project. Ask yourself, "What do we need to accomplish with the implementation of Configuration Manager?" and try to answer this question with the help of your colleagues.

While planning a Configuration Manager environment you can schedule a workshop to define the scope and expectations of your project. You want the results to be accepted by your colleagues or customer. You also need to think from the users' perspective since Configuration Manager 2012 placed the user in the center. User-centricity is new but can be very powerful and well adopted by your organization or customer. During the workshop try to answer the following questions:

- Does the Configuration Manager 2012 environment need to have high availability?
- How is your IT management organized? Do you need role-based administration, or are all the administrators allowed to perform every task?
- How is your organization organized?
- Do you need to implement or do you support a full application lifecycle model?
- What kind of devices are you going to support? Which level of support do you want to provide?

- Are there relationships between users and systems?
- Do you deploy operating systems? If so, where do you need to deploy them?
- Would you like to implement self-service for the end users?
- Are you going to use one set of client settings, or is there a need for client settings based on collections of users or devices?
- Will you need to use the remote management features of Configuration Manager? If so, for what devices?
- Is there a need to use hardware and software inventory and asset intelligence?
- Is there a service-level agreement available that must be met after the implementation?

Describing the Network

When planning a Configuration Manager infrastructure, you want to look at your current network design. Collect as much information as you can about your current Configuration Manager 2007 infrastructure, your Active Directory, and your network design; this can help you make the right design decisions.

Think about the following when describing the network:

- Make a diagram of your network. The diagram must include the following: LAN and WAN infrastructure, network size per location, available bandwidth, network latency, and the use of firewalls.
- Do Configuration Manager clients need to connect to the Configuration Manager site from the Internet?
- Are you allowed to extend Active Directory with the Configuration Manager schema?
- Document your IPv4 and IPv6 number plan.
- Describe your Active Directory forest structure and possible Active Directory trusts.
- Describe your Active Directory organizational unit structure; where are your assets?
- Describe your security demands. Does Configuration Manager need to be configured to support HTTP or HTTPS intranet connections or both? Is a public key infrastructure available?
- Describe your servers and roles; if you want to manage your servers with Configuration Manager 2012, it's good to define different maintenance windows per groups of servers.
- Do you already use Windows Server Update Services in your environment? Can it be replaced by Configuration Manager 2012?

Describing Your Migration Needs

With the migration feature in Configuration Manager 2012 you need to really think about how you want to migrate the investments you made in Configuration Manager 2007.

There is only one supported scenario for migrating to Configuration Manager 2012; this is a side-by-side scenario. You need to list which collections, applications, software update deployments, operating systems, and other objects you want to migrate.

Define up front how long you want to keep the two environments operational since you need to administer two Configuration Manager infrastructures and possibly re-migrate objects you migrated earlier in the process.

Planning the Configuration Manager Environment

In order to plan, design, and implement a Configuration Manager 2012 environment, you need to take several steps to be able to implement it in the right way for your business. Configuration Manager 2012 can be installed and configured in many different ways, and you must make many design decisions.

Plan a workshop with your Configuration Manager team to make decisions about the following subjects:

- System requirements
- Active Directory considerations
- Hierarchies and sites
- Site boundaries and boundary groups
- Site system roles
- Site communications
- Site security
- Discovery of your resources
- Client settings and client deployment
- Content management
- Role-based administration
- Migration
- Disaster recovery

System Requirements

When planning your Configuration Manager 2012 infrastructure, you need to define what kind of hardware and software your infrastructure will use and what kind of devices you want to manage via the Configuration Manager 2012 infrastructure. This section describes the hardware and software requirements for the Configuration Manager 2012 infrastructure.

Configuration Manager Client Requirements

Configuration Manager 2012 supports managing various clients with various operating systems. In addition to the Windows operating systems, Configuration Manager now also supports

mobile device operating systems. In the tables in this section you will find the supported client operating systems.

Hardware

The minimum and recommended hardware requirements for the Configuration Manager 2012 clients are shown in Table 2.1. Refer to the processor and RAM requirements for the operating systems of the devices.

Table 2.1: Hardware requirements/recommended

Component	Requirement	Recommended
Free disk space for client	500 MB	In addition to the required 500 MB, another 5 GB of free space for the client cache
RAM for operating system deployment	384 MB	
Software center	500 MHz processor	
Remote control	Pentium 4 HT 3 GHz or higher and 1 GB of RAM for best experience	
Out-of-band management	Support for Intel vPro technology or Intel Centrino Pro and a supported version of Intel AMT	

Operating System

Configuration Manager 2012 supports various operating systems for desktops, laptops, and mobile devices. Windows versions ranging from Windows XP to Windows 8.1, plus Windows Server, Windows Mobile, and Nokia Symbian are supported by Configuration Manager 2012. The exact versions and editions are found in the tables of this section.

Windows XP

Windows XP is still a very popular operating system and is well used in a lot of environments. As well as normal operating system versions, the operating systems for tablet and embedded devices are supported. Windows XP is supported until April 4, 2014, so be sure to read Chapter 10, "Operating System Deployment," and see how you are able to migrate your Windows XP SP3 computers to a later version of Windows. Table 2.2 lists the supported versions.

TABLE 2.2: Supported Windows XP versions

WINDOWS XP VERSION	X86	X64
Professional Service Pack 3	✓	
Professional for 64-bit systems Service Pack 2		✓
Windows XP Tablet PC (SP3)		
Windows Embedded Standard 2009 (based on Windows XP SP3)	✓	
Windows XP Embedded SP3 (based on Windows XP SP3)	✓	
Windows Fundamentals for Legacy PCs (WinFLP) (based on Windows XP SP3)	✓	
Windows Embedded POSReady 2009 (based on Windows XP SP3)	✓	
WEPOS 1.1 SP3 (based on Windows XP SP3)	✓	

Windows Vista

Configuration Manager 2012 is able to manage Windows Vista versions as of Service Pack 2. If you still have the RTM version of Windows Vista or earlier Service Pack releases, you need to install Service Pack 2 before the Configuration Manager 2012 client can be installed. Table 2.3 shows the supported Windows Vista versions.

TABLE 2.3: Supported Windows Vista versions

WINDOWS VISTA VERSION	X86	X64
Business Edition Service Pack 2	✓	✓
Enterprise Edition Service Pack 2	✓	✓
Ultimate Edition Service Pack 2	✓	✓

Windows 7

Table 2.4 shows you the Windows 7 editions that are supported by Configuration Manager 2012.

TABLE 2.4: Supported Windows 7 versions

WINDOWS 7 VERSION	X86	X64
Enterprise Edition	✓	✓
Ultimate Edition	✓	✓
Professional Edition	✓	✓

Windows 7 version	x86	x64
Enterprise Edition Service Pack 1	✓	✓
Ultimate Edition Service Pack 1	✓	✓
Professional Edition Service Pack 1	✓	✓
Windows Embedded Standard 7	✓	✓
Windows Embedded POSReady 7	✓	✓
Windows Thin PC	✓	✓

Windows 8 and Windows 8.1

The market share of Windows 8.1 is getting bigger. Table 2.5 shows you which editions are supported by Configuration Manager 2012 and how.

Table 2.5: Supported Windows 8 versions

Versions	x86	x64	Client
Windows 8 Enterprise Edition	✓	✓	Full / OMA-URI
Windows 8 Pro	✓	✓	Full / OMA-URI
Windows 8.1 Enterprise Edition	✓	✓	Full / OMA-URI
Windows 8.1 Pro	✓	✓	Full / OMA-URI
Windows RT	✓	✓	OMA-URI
Windows 8.1 RT	✓	✓	OMA-URI
Windows Embedded 8 Pro	✓	✓	Full
Windows Embedded 8	✓	✓	Full
Standard	✓	✓	Full
Windows Embedded 8	✓	✓	Full
Industry	✓	✓	Full
Windows Embedded 8.1	✓	✓	Full
Industry	✓	✓	Full

Windows Server 2003

Windows Server 2003 is also well used in IT environments. Configuration Manager 2012 supports Windows Server 2003 as of Service Pack 2 and the R2 version. Table 2.6 shows you the complete list of supported versions.

TABLE 2.6: Supported Windows Server 2003 versions

WINDOWS SERVER 2003 VERSION	X86	X64
Web Edition Service Pack 2	✓	
Enterprise Edition Service Pack 2	✓	✓
Datacenter Edition Service Pack 2	✓	✓
Standard Edition R2 SP2	✓	✓
Enterprise Edition R2 SP2	✓	✓
Datacenter Edition R2 SP2	✓	✓
Storage Server Edition R2 SP2	✓	✓

Windows Server 2008

Windows Server 2008 comes in different editions and for different platforms. Table 2.7 provides the complete list of supported versions and editions.

TABLE 2.7: Supported Windows Server 2008 versions

WINDOWS SERVER 2008 VERSION	X86	X64
Standard Edition Service Pack 2	✓	✓
Enterprise Edition Service Pack 2	✓	✓
Datacenter Edition Service Pack 2	✓	✓
R2 Standard Edition (core and full)		✓
R2 Enterprise Edition (core and full)		✓
R2 Datacenter Edition (core and full)		✓
R2 Standard Edition Service Pack 1 (core and full)		✓
R2 Enterprise Edition Service Pack 1 (core and full)		✓
R2 Datacenter Edition Service Pack 1 (core and full)		✓

Windows Server 2012 (R2)

The new flagship of Microsoft Windows Server 2012 R2 comes in different versions. Table 2.8 shows you which editions are supported by Configuration Manager 2012.

Table 2.8: Supported Windows Server 2012 R2 versions

Versions	X64
Windows Server 2012 Standard	✓
Windows Server 2012 Datacenter	✓
Windows Server 2012 R2 Standard	✓
Windows Server 2012 R2 Datacenter	✓
Windows Server 2012 Core installation	✓
Windows Server 2012 R2 Core installation	✓

Datacenter Releases Are Supported But Not Certified

The Datacenter versions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 are supported but not certified for Configuration Manager 2012.

Apple Mac OS X

Configuration Manager 2012 R2 supports a broad range of Windows, Linux, and Mac devices. Table 2.9 lists the supported Mac OS X operating systems.

Table 2.9: Supported Mac OS X versions

Versions	Supported
Mac OS X 10.6	✓
Mac OS X 10.7	✓
Mac OS X 10.8	✓

Linux and Unix Operating Systems

The Linux and Unix operating systems are the odd-men-out operating systems that are supported by Configuration Manager 2012 R2, since they are server-based operating systems only. In Table 2.10 you can see which versions are supported.

TABLE 2.10: Supported Linux and Unix versions

VERSIONS	VERSION	SUPPORTED
Red Hat Enterprise Linux	4 x86	✓
Red Hat Enterprise Linux	4 x64	✓
Red Hat Enterprise Linux	5 x86	✓
Red Hat Enterprise Linux	5 x64	✓
Red Hat Enterprise Linux	6 x86	✓
Red Hat Enterprise Linux	6 x64	✓
Solaris	9 SPARC	✓
Solaris	10 x86	✓
Solaris	10 SPARC	✓
Solaris	11 x86	✓
Solaris	11 SPARC	✓
SUSE Linux Enterprise Server	9 x86	✓
SUSE Linux Enterprise Server	10 x86 SP1	✓
SUSE Linux Enterprise Server	10 x64 SP1	✓
SUSE Linux Enterprise Server	11 x86 SP1	✓
SUSE Linux Enterprise Server	11 x64 SP1	✓
CentOS	5 x86	✓
CentOS	5 x64	✓
CentOS	6 x86	✓
CentOS	6 x64	✓
Debian	5 x86	✓
Debian	5 x64	✓
Debian	6 x86	✓
Debian	6 x64	✓
Debian	7 x86	✓

Versions	Version	Supported
Debian	7 x64	✓
Ubuntu	10.4 LTS x86	✓
Ubuntu	10.4 LTS x64	✓
Ubuntu	12.4 LTS x86	✓
Ubuntu	12.4 LTS x64	✓
Oracle Linux	5 x86	✓
Oracle Linux	5 x64	✓
Oracle Linux	6 x86	✓
Oracle Linux	6 x64	✓
HP-UX	11iv2 IA64	✓
HP-UX	11iv2 PA-RISC	✓
HP-UX	11iv3 IA64	✓
HP-UX	11iv3 PA-RISC	✓
AIX	5.3 Power	✓
AIX	6.1 Power	✓
AIX	7.1 Power	✓

Operating Systems for Mobile Phones and Handheld Devices

Configuration Manager 2012 supports management for several mobile phones and handheld devices. The level of support and the features vary per platform and client type, but each platform supports inventory, settings management, and software deployment. The support can be divided into two levels:

- Depth management
- Light management

Devices that are supported through depth management are enrolled in Configuration Manager 2012 and receive a Configuration Manager 2012 client, or the mobile devices can be enrolled into Configuration Manager 2012 via the Windows Intune connector. To be able to support the light management of devices, you need to connect the Configuration Manager 2012 environment to a Microsoft Exchange Server 2010 (SP1) or higher on-premises or online environment. In Chapter 16, "Mobile Device Management," you can find the supported features and the supported mobile devices and learn how to enroll the mobile devices into Configuration Manager 2012 R2.

Configuration Manager Site Server Requirements

The Configuration Manager site server roles can be installed on different kinds of hardware and software platforms. This section will help you to identify the hardware and software options you have when planning your site servers.

Hardware

In Table 2.11 you will find the minimum and recommended hardware requirements for Configuration Manager site systems. Be sure that the hardware supports a 64-bit operating system. The only exception is for the distribution point site role; this role can be installed on a limited list of 32-bit operating systems. The following requirements are based on the requirements of Windows 2008 SP2 x64.

Table 2.11: Hardware requirements/recommended

Component	Requirement	Recommended
Processor	1.4 GHz processor	2.0 GHz or faster
RAM	4 GB	8 GB or more
Free disk space	10 GB	50 GB (if using operating system deployment)

In many cases you will need fewer servers than with earlier versions and have less resource waste.

Software Requirements for Site System Roles

To be able to install and configure Configuration Manager 2012 site system roles on your servers, the operating system must comply with some requirements. Site system roles are roles that can be installed and configured on Configuration Manager 2012 site systems. This section will describe the requirements for installing the different site system roles.

Operating Systems

Depending on the roles you want to install, you can choose which operating system you want to install the site system role on. Every site system role has certain requirements for which operating system it can be installed on. For instance, a management point site system role can be installed only on a 64-bit Windows Server operating system in contrast to the distribution point site system role, which is supported on a large number of operating systems. This section helps you to identify the operating system requirements for site system roles.

Site System Roles with the Same Operating System Requirements

Most site system roles require the same operating systems. The following site server roles have the same OS requirements:

- Central administration site
- Primary site server
- Secondary site server
- Site database server
- SMS provider
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Management point
- Application Catalog web service point
- Application Catalog website point
- Asset Intelligence synchronization point
- Endpoint Protection point
- Out of band service point
- Reporting services point
- Software update point
- State migration point
- System health validator point

The operating system versions in Table 2.12 support installing the site roles mentioned here.

TABLE 2.12: Supported operating systems

OPERATING SYSTEM	X86	X64
Windows Server 2008 Standard Edition (SP2)		✓
Windows Server 2008 Enterprise Edition (SP2)		✓
Windows Server 2008 Datacenter Edition (SP2)		✓
Windows Server 2008 R2 Standard Edition		✓
Windows Server 2008 R2 Enterprise Edition		✓
Windows Server 2008 R2 Datacenter Edition		✓
Windows Server 2008 R2 SP1 Standard Edition		✓
Windows Server 2008 R2 SP1 Enterprise Edition		✓

TABLE 2.12: Supported operating systems *(CONTINUED)*

OPERATING SYSTEM	X86	X64
Windows Server 2008 R2 SP1 Datacenter Edition		✓
Windows Server 2012 Standard		✓
Windows Server 2012 Datacenter		✓
Windows Server 2012 R2 Standard		✓
Windows Server 2012 R2 Datacenter		✓
Windows Server 2012 Foundation		✓
Windows Server 2012 R2 Foundation		✓

The site system roles are not supported on a Core installation of Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 Foundation, Windows Server 2008 R2 Foundation, Windows Server 2012, or Windows Server 2012 R2 editions.

Some of the site server roles can be installed on different operating systems than the ones required for the roles listed previously. The following site server roles can be installed and configured on many more operating systems:

- Distribution point
- Client status reporting host system

The operating systems that are supported for the distribution points are listed in Table 2.13. The support of distribution points on Windows Server 2003 has some feature limits. For instance, BranchCache will not work with Windows Server 2003.

TABLE 2.13: Supported operating systems for distribution points

OPERATING SYSTEM	X86	X64
Windows Vista Business Edition 64-bit SP1		✓
Windows Vista Enterprise Edition 64-bit SP1		✓
Windows Vista Ultimate Edition 64-bit SP1		✓
Windows Server 2003 Standard Edition R2	✓	✓
Windows Server 2003 Enterprise Edition R2	✓	✓
Windows Server 2003 Web Edition SP2	✓	
Windows Server 2003 Standard Edition SP2	✓	✓
Windows Server 2003 Enterprise Edition SP2	✓	✓

Operating System	x86	x64
Windows Server 2003 Datacenter Edition SP2	✓	✓
Windows Server 2003 Storage Server Edition SP2	✓	
Windows Server 2008 Standard Edition (SP2)	✓	✓
Windows Server 2008 Enterprise Edition (SP2)	✓	✓
Windows Server 2008 Datacenter Edition (SP2)	✓	✓
Windows Server 2008 R2 Standard Edition		✓
Windows Server 2008 R2 Enterprise Edition		✓
Windows Server 2008 R2 Datacenter Edition		✓
Windows Server 2008 R2 SP1 Standard Edition		✓
Windows Server 2008 R2 SP1 Enterprise Edition		✓
Windows Server 2008 R2 SP1 Datacenter Edition		✓
Windows Storage Server 2008 R2 Workgroup		✓
Windows Storage Server 2008 R2 Standard		✓
Windows Storage Server 2008 R2 Enterprise		✓
Windows Server 2012 Standard		✓
Windows Server 2012 Datacenter		✓
Windows Server 2012 R2 Standard		✓
Windows Server 2012 R2 Datacenter		☒
Windows 7 Professional Edition (with or without SP1)	✓	✓
Windows 7 Enterprise Edition (with or without SP1)	✓	✓
Windows 7 Ultimate Edition (with or without SP1)	✓	✓
Windows 8 Professional	✓	✓
Windows 8 Enterprise	✓	✓
Windows 8.1 Professional	✓	✓
Windows 8.1 Enterprise	✓	✓

When using Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows Server 2003 R2 platforms, only the standard distribution point is supported. Enhanced features like

PXE or Multicast are not supported. When using Windows Server 2008 SP2 Multicast on the Distribution Point is not supported.

Prerequisite Software Requirements

The following software must be installed and, if needed, configured before you can install Configuration Manager 2012:

- Windows Server Update Services 3.0 SP2
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4 (for Windows Server 2008)
- Microsoft .NET Framework 4.5 (of Windows Server 2012)
- Active Directory schema extended with Configuration Manager 2012 classes
- Windows ADK 8.1

The following SQL Server versions are supported:

- SQL Server 2008 SP2 (Standard or Enterprise) with a minimum of Cumulative Update 9
- SQL Server 2008 SP3 (Standard or Enterprise) with a minimum of Cumulative Update 4
- SQL Server 2008 R2 (Standard or Enterprise) with SP1 with a minimum of Cumulative Update 6
- SQL Server 2008 R2 (Standard or Enterprise) with SP2
- SQL Server 2012 (Standard or Enterprise) with a minimum of Cumulative Update 2
- SQL Server 2012 (Standard or Enterprise) with SP1
- SQL Server Express 2008 R2 with SP1 with a minimum of Cumulative Update 6 (secondary sites only)
- SQL Server Express 2008 R2 with SP2 (secondary sites only)
- SQL Server Express 2012 and a minimum of Cumulative Update 2 (secondary sites only)
- SQL Server Express 2012 with SP1 (secondary sites only)

The collation of the SQL Server and the site databases must be SQL_Latin1_General_CP1_CI_AS to be able to install Configuration Manager 2012 R2.

As with Configuration Manager 2007, several roles and features of Windows Server need to be installed and configured:

- Background Intelligent Transfer Service (BITS)
- Remote Differential Compression
- IIS7 (with IIS6 Management compatibility, ASP.NET, Static Content Compression, and the common IIS and security features)

We'll discuss more on the installation of Configuration Manager 2012 in Chapter 4, "Installation and Site Role Configuration."

Extending the Active Directory Schema

When you are migrating from Configuration Manager 2007 and you already have extended the Active Directory schema, you do not have to extend it again. The Active Directory schema of Configuration Manager 2007 is the same for Configuration Manager 2012. The schema extensions for Configuration Manager 2012 are unchanged.

When planning the extension of the Active Directory schema for Configuration Manager 2012, you need to take into account that several site roles require the extension.

Extending Active Directory is not part of the installation process; when extending you can publish the Configuration Manager site information into Active Directory automatically. Extending the Active Directory schema is done by executing a separate executable; you can find more about this procedure in Chapter 4.

Extending the Active Directory schema is optional, but for some features extending it is required. Table 2.14 provides the list of Configuration Manager 2012 features that require an extended Active Directory schema or need it optionally.

Table 2.14: Configuration Manager 2012 features that require an extended Active Directory schema

Feature	Schema Extension	Description
Client installation	Optional	When installing or pushing a new Configuration Manager client, the client will default search Active Directory for information about the Configuration Manager 2012 environment. Searching Active Directory provides such information as where the management point resides and the Configuration Manager site name. If you don't want to extend Active Directory, you can install the client with installation parameters such as SMSMP, or you can publish the management point in DNS and in WINS.
Automatic site assignments/global roaming	Optional	If you don't want to extend Active Directory, you need to publish the management point in WINS. Otherwise, the Configuration Manager client won't find the management point and cannot communicate with the site servers.
TCP port configuration for client-to-server communication	Optional	When you install a Configuration Manager client, it is configured with information about the TCP ports that are used to communicate with the site servers.
Network Access Protection	Required	Configuration Manager publishes health state information to Active Directory; this way the system health validator point can validate whether a client is healthy.

Microsoft best practice is to extend Active Directory with the Configuration Manager schema. Also be sure that the primary site servers have access to the Systems Management container in Active Directory.

Hierarchies and Sites

When planning for a Configuration Manager 2012 infrastructure, you need to have a clear understanding of what your global network infrastructure looks like; also, you need to take into account your business needs. The Configuration Manager 2012 architecture is simplified from earlier versions and consists of the following site types:

- Central Administration Site
- Primary site
- Secondary site

Next to the site types, a distribution point can have an essential role in the Configuration Manager hierarchy. A Configuration Manager hierarchy consists of Configuration Manager sites that are linked directly or indirectly and have a parent-child relationship, as shown in Figure 2.1.

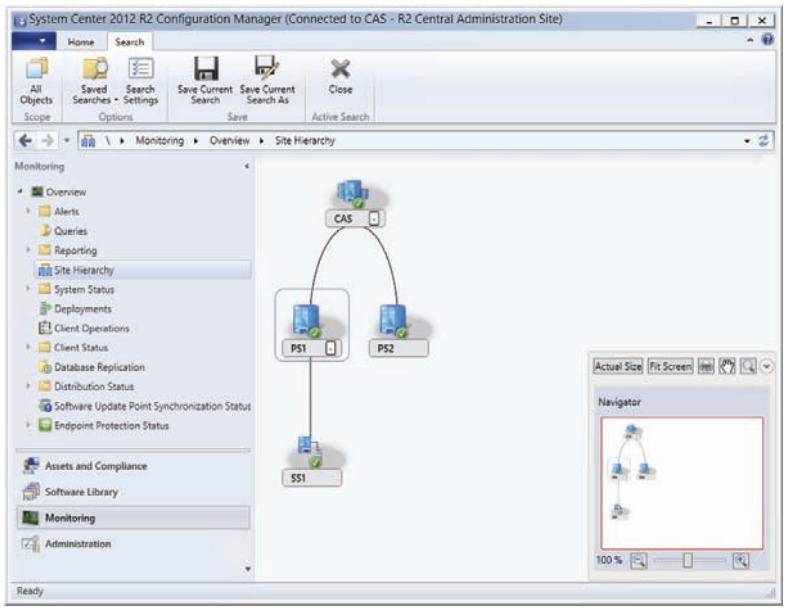


Figure 2.1
A Configuration Manager hierarchy

Central Administration Site

The Central Administration Site (CAS) is the top-level site in a Configuration Manager hierarchy and is the recommended location for all administration and reporting for a Configuration Manager 2012 hierarchy. It has limited site roles available, has no clients assigned, and doesn't process client data.

The CAS supports only primary sites as child sites. When you are using two or more primary sites, a CAS is always the first site you need to install. A primary site that is installed before implementing a CAS cannot be attached to the CAS. A SQL server is needed for data that is gathered from the hierarchy. The data includes such information as inventory data and status messages from the hierarchy. You can configure the discovery of objects in the hierarchy from the CAS by assigning discovery methods to run in individual sites in the hierarchy.

The following site roles can be configured for Central Administration Sites:

- System health validator point
- Software update point
- Asset Intelligence synchronization point
- Reporting Services point
- Endpoint Protection point
- Certificate Registration point
- Windows Intune connector

A Central Administration Site can support up to 25 child primary sites.

Primary Site

The primary site serves clients in well-connected networks. A primary site can have a CAS as its parent tier. A primary site cannot have another primary site as its parent tier. Since role-based administration is a real feature, no separate primary sites are needed for security, administrative, or data-segmentation purposes.

Extra primary sites can be added for the following reasons:

- Managing clients directly
- Providing a local point for administration
- Supporting more than 100,000 clients

The following are design rules for primary sites:

- Primary sites can be stand-alone or members of a hierarchy.
- A primary site cannot change its parent site relationship after the installation.
- A stand-alone primary site cannot be assigned to a Central Administration Site after the installation, but you can install an empty CAS above the stand-alone primary site.
- Primary sites that are installed as children of a CAS will configure database replication to the parent site automatically.
- Primary sites use database replication for the communication to their child and parent sites.
- Primary sites can have only a central administration point as a parent site.
- Primary sites can support one or more secondary sites as child sites.
- Primary sites process all client data from their assigned Configuration Manager clients.

- A primary site can support up to 10 management points for load balancing.
- A primary site can support up to 250 secondary sites.

The following site roles can be configured for primary site servers:

- Management point
- Distribution point
- Software update point
- System health validator point
- State migration point
- Fallback status point
- Out-of-band service point
- Asset Intelligence synchronization point (only on stand-alone primary site)
- Reporting Services point
- Application Catalog web service point
- Application Catalog website point
- Enrollment proxy point
- Enrollment point
- Certificate registration point
- Endpoint Protection point (only on stand-alone primary site)
- Windows Intune connector (only on stand-alone primary site)

Secondary Site

A secondary site is installed through the Configuration Management console. The site can be used to service clients in remote locations where network control is needed. You can use secondary sites for servicing site roles such as software update points, PXE-enabled distribution points, and state migration points and if you need tiered content routing for deep network topologies.

Reassigning a secondary site to another primary site is not possible; you need to delete the secondary site and reinstall it from the Configuration Manager console.

The following are design rules for secondary sites:

- When installing a secondary site, it will automatically install SQL Server Express if a local SQL Server is not available.
- Secondary sites that are installed as children of a primary site will configure database replication to the parent site automatically.
- Secondary sites use database replication for the communication to their parent sites and receive a subset of the Configuration Manager database.
- Secondary sites support the routing of file-based content between secondary sites.

- When installing secondary sites, a management point and a distribution point are installed automatically.
- Upward and downward flow of data is required.

The following site roles can be configured for secondary site servers:

- Management point
- Distribution point
- Software update point
- State migration point

Distribution Points

Distribution point is the Configuration Manager role that stages packages to clients. The distribution point role is more enhanced than in earlier versions. In Configuration Manager 2012, the old standard, server share, and branch distribution points are merged into one distribution point role.

The following are design rules for distribution points on a remote site without a local primary site or secondary site server present:

- The bandwidth of your network is sufficient to communicate and send and receive information such as client inventory, client policies, reporting status, or discovery information to or from a management point.
- Background Intelligent Transfer Service does not provide enough bandwidth control for your network environment.
- You need to stream virtual applications to clients at a remote location.
- You need to use the multicast protocol for deploying operating systems to clients at a remote location.
- You need downward flow of data.

If these rules do not apply and a primary site or secondary site is also not needed, your clients can probably use a remote distribution point.

A distribution point cannot be connected to a central administration point; it always communicates with a primary site or a secondary site.

The distribution point role now supports the following:

- Scheduling and throttling of data synchronization
- PXE
- Multicast
- Content library
- Content validation
- State-based distribution point groups
- Prestaged content
- BranchCache

These are described in detail in the following sections.

Scheduling and Throttling

Whereas in Configuration Manager 2007 you needed a secondary site to be able to manage the synchronization of data on the distribution points, you are now able to control content distribution by using bandwidth, bandwidth throttling, and scheduling options. With scheduling you are able to define periods for restricting synchronization traffic to the distribution point. You can configure synchronizations per day, per hour, and by priority. With throttling you are able to configure options like the following:

Unlimited When Sending To This Destination When you choose this option, all available bandwidth will be used for distribution point synchronization traffic.

Limited To Specified Maximum Transfer Rates By Hour Configure per hour the percentage of the bandwidth that is allowed to be used for distribution point synchronization traffic.

Pulse Mode When you choose this option, you can define the block size of the data that needs to be synchronized and the time delay between each block that is sent to the distribution point.

Scheduling and throttling are available only on site systems with only the distribution point site role installed.

PXE

To be able to install operating systems in your environment, you need to configure PXE support. PXE support allows you to boot into a boot image that is used to initiate operating system deployment for Configuration Manager 2012 clients. With Configuration Manager 2012, this role is moved from the site server to a server with the distribution point available. Per site, up to 250 PXE-enabled distribution points are supported.

Multicast

The multicast support is used to deploy operating systems while conserving network bandwidth by simultaneously sending data to multiple clients instead of sending data to each client using a separate session.

Best practice is that the same distribution point is not used for multicast and unicast distributions at the same time.

Content Library

The way of storing data on the distribution point has changed drastically; where Configuration Manager 2007 stored a lot of duplicate content, Configuration Manager 2012 stores content only once. The content is stored in the content library (SCCMContentLib). This library is divided in three parts:

Data Library (DataLib) The data library holds INI files with metadata information about each file in the file library.

File Library (FileLib) The file library holds the actual files of the packages. It provides single-instance storage of files on the site server and distribution point.

Package Library (PkgLib) The package library stores information about the content in each package.

The content library replaces the compressed content on the Configuration Manager 2007 distribution points and replaces the smspk*x*$ share (where *x* represents the volume name hosting the share), the place where the compressed content was stored.

For site-to-site replication of distribution point content, compressed copies of the content are still used. The compression method is new and has a higher compression rate. A new component called PkgXferMgr performs the distribution.

The location of the distribution point share can be spanned over different drives. Drives will have a priority set for file storage, instead of the drive with the most space being used like in earlier versions.

Content Validation

A new feature in Configuration Manager 2012 is the ability to validate the content on a distribution point (see Figure 2.2). When validating the content on a distribution point, the validation process will check to see if the content on the distribution point is the same as the content in the source of the application or package. Validating the content can be scheduled for the distribution point or done per package.

Per application on the distribution point, you are able to validate, redistribute, or remove the content. If the content is not valid, it will then be reported in the Content Status node in the Monitoring workspace of the Configuration Manager console.

State-Based Distribution Point Groups

In Configuration Manager 2007, distribution point groups were just for administrative purposes to easily target software, but in Configuration Manager 2012, the concept has changed. The distribution point groups are state based; this means that when you add a distribution point to a group, it will receive all the content that has previously been assigned to the distribution point group.

Content Prestaging

A new feature that replaces the courier senders and the package preload tool used in earlier versions of Configuration Manager is called Content Prestage. The courier senders and the package preload tool were used to provide distribution points with content from a physical medium (DVD, tape, external disk, and so on) instead of synchronizing the content over the WAN. The feature allows you also to deploy a remote distribution point without using the WAN to let it synchronize with the site server in the hierarchy. With Content Prestage you are able to save content to an offline media device and load it locally on the remote distribution point.

BranchCache

Since Configuration Manager 2007 SP2, distribution points also support a feature of Windows Server 2008 R2 called BranchCache. BranchCache is used to reduce WAN utilization and enhance access to content at the central office from branch office locations. When BranchCache is enabled, a copy of content retrieved from a server is cached in the branch office. When someone else wants to retrieve the same content, the client will retrieve the content from the cache available in the branch office; this way the WAN is not used to get the content again from the centrally located server. This BranchCache feature caches HTTP, HTTPS, BITS, or SMB-based content on both distributed cache and local cache locations. A distributed cache is a cache location on a Windows 7 client that is configured to use BranchCache. A local cache is a location on a Windows 2008 R2 server in the branch office where BranchCache is enabled.

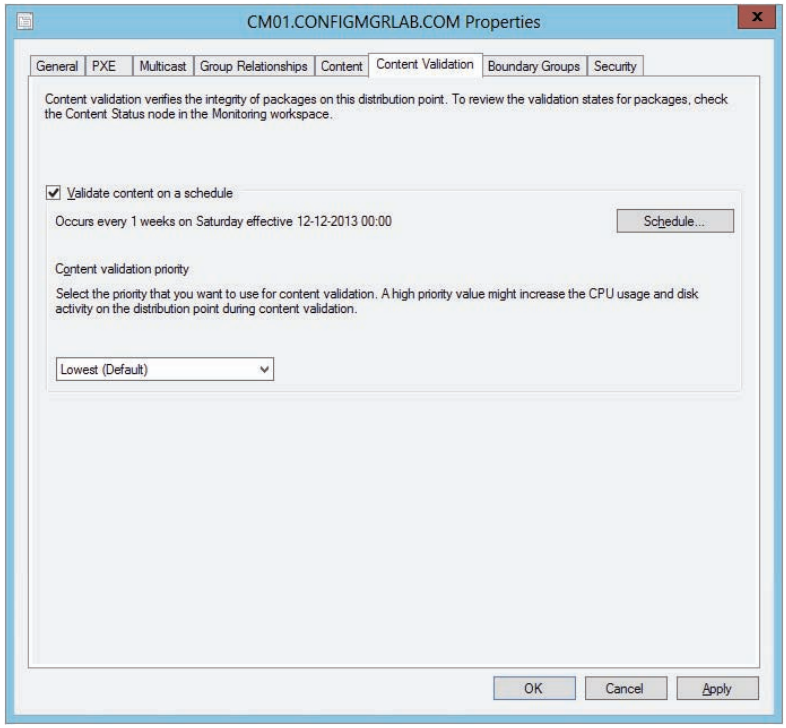


FIGURE 2.2 Managing the content on the distribution point

There is no special configuration option in Configuration Manager 2012 to enable BranchCache since it is not a feature of Configuration Manager 2012. The only thing you need to configure is that your deployments are enabled for downloading and running the applications locally.

BranchCache is often used in WAN environments with a lot of latency and with slow data links between the sites.

BranchCache works only in a combination of Windows 7 clients and Windows Server 2008 R2.

Site Boundaries and Boundary Groups

In Configuration Manager 2012 you can define one or more network locations called *boundaries*. A boundary in Configuration Manager 2012 can be based on the following types:

IP Subnet A boundary can be a subnet ID, which is automatically calculated while entering the IP subnet and subnet mask.

Active Directory Site When you are using Active Directory sites in your Active Directory domain, you can configure the boundary to use an Active Directory site.

IPv6 Prefix If you are configuring Configuration Manager 2012 in an IPv6 environment, you can configure a boundary to use an IPv6 prefix. An IPv6 prefix is a fixed part of the IPv6 address or the network ID.

IP Address Range Instead of using an IP subnet, you can configure the boundary to use an IP address range. The IP address range can be defined according to your needs.

The boundaries can contain devices that you want to manage with Configuration Manager 2012. Each boundary must be a member of one or more boundary groups, which are collections of boundaries. Boundaries are available for the Configuration Manager 2012 hierarchy, whereas boundaries in Configuration Manager 2007 were site specific.

New for clients is that before clients can identify an assigned site or locate content on a distribution point, a boundary must be associated with a boundary group. The boundary group is used for clients to find their assigned site, and they are used to locate content. In a boundary group you can associate system servers that have distribution points or state migration points installed so that the client can find software like applications, operating system images, and software updates. Boundary groups can be added to keep boundaries organized in a logical way.

Boundary creation can be done by hand, but when you enable the Active Directory Forest Discovery feature, you can create Active Directory site boundaries and IP subnet boundaries automatically at the same time. This process can be configured to run periodically. When migrating from Configuration Manager 2007, boundaries and boundary groups are also automatically created during the migration process.

Configuring Network Speed

In Configuration Manager 2007, you needed to configure the network speed for your location. In Configuration Manager 2012, you need to configure the network speed on the Content Location property per distribution point in a boundary group.

A boundary group can be assigned to a specific site and can have one or more content locations. A distribution point can be added to one or more boundary groups. The boundary groups will provide the clients with a list of distribution points to download the content from. The client will choose the nearest distribution point.

Do Not Overlap Boundaries

When planning boundary groups, avoid overlapping the boundaries. This is allowed in Configuration Manager 2012 and earlier versions, but when you use automatic site assignment, the site that a client will be assigned to is unpredictable. So do not use overlapping in combination with automatic client assignment.

Site System Roles

Site system roles are roles that can be installed on Configuration Manager 2012 site servers. Depending on the size of your site and hardware, you can assign multiple roles to one site system server. Some site system roles are installed while installing Configuration Manager 2012 or when adding a secondary site to the Configuration Manager 2012 infrastructure. Others can be installed in the Configuration Manager console.

The following list provides an overview (in alphabetical order) of all the site roles and what they are used for. More information about the site system roles can be found in Chapter 4.

Application Catalog Web Service Point The Application Catalog web service point publishes software information from the software library to the Application Catalog website. This site role is available hierarchy wide.

Application Catalog Website Point The Application Catalog website point publishes the available software for a user, depending on the user rights. The Application Catalog website allows users with mobile devices to remotely wipe their device or request software that is available for distribution but not without approval from the system administrator. This site role is available hierarchy wide.

Asset Intelligence Synchronization Point The Asset Intelligence synchronization point synchronizes the Asset Intelligence Catalog information with the System Center online service. This site system role can only be installed on the Central Administration Site server in a hierarchy or a stand-alone primary site server. Synchronization of the Asset Intelligence information can be scheduled or run manually. This site role is available hierarchy wide.

Certificate Registration Point The certificate registration point communicates with the server that runs the Network Device Enrollment Service of Active Directory Certificate Services to manage device certificate requests that use the Simple Certificate Enrollment Protocol (SCEP).

Component Server A component server is automatically installed with all site system roles except the distribution point and is used to run Configuration Manager services.

Distribution Point Distribution point is the Configuration Manager role that stages packages such as application content, software packages, software updates, operating system images, and boot images to clients. The distribution point role in Configuration Manager 2012 also supports PXE, scheduling, bandwidth throttling, multicast, and content validation. This site role is available only in the site.

Endpoint Protection Point The Endpoint Protection role integrates the former Forefront Endpoint Protection with Configuration Manager 2012. The role is configured at the Central Administration Site or a stand-alone primary site. With the System Center Endpoint Protection role you can secure your clients and servers from viruses and malware. To be able to use the Endpoint Protection point, you need to accept the license terms and configure the default membership for the Microsoft Active Protection Service.

Enrollment Point When implementing mobile device management or secure out-of-band management, an enrollment point is needed. Public key infrastructure (PKI) certificates are required to complete the enrollment of the mobile device, and the device will provision AMT-based clients. This site role is available only in the site.

Enrollment Proxy Point When implementing mobile device management, an enrollment proxy point is needed to manage enrollment requests from mobile devices. Mobile device enrollment will need a PKI to secure the over-the-air communication with the mobile devices. This site role is available only in the site.

Fallback Status Point When a client becomes unmanaged or the management point is unable to communicate with the client, a fallback status point will point out unmanaged clients and helps you monitor the client installation. This site role is available hierarchy wide.

Management Point The management point provides policy and content location information to Configuration Manager clients. It also receives configuration data from Configuration Manager clients.

The server locator point functionality as it is known in Configuration Manager 2007 is moved to the management point. If the Configuration Manager client is no longer able to retrieve site information from Active Directory or WINS, the management point is used to provide this information.

This site role is available only in the site.

Out-of-Band Service Point The out-of-band service point is used for provisioning and configuring AMT-based computers for out-of-band management. This site role is available only in the site.

Reporting Services Point For reporting you need a Reporting Services point; this role integrates with SQL Server Reporting Services. You can create and manage reports for Configuration Manager. This site role is available hierarchy wide.

Site Database Server The site database server hosts the Microsoft SQL Server database. This database is used to store information about assets and site data.

SMS Provider This is installed automatically when you install a Central Administration Site and when you install a primary site. The SMS provider is the interface between the Configuration Manager 2012 console and the Configuration Manager 2012 database. Secondary sites do not install SMS providers.

Software Update Point The software update point is used for integration with Windows Server Update Services so that software updates can be deployed and managed with Configuration Manager. This site role is available only in the site.

State Migration Point When a computer receives a new operating system, the user state will be stored at the state migration point. The state migration point receives the user state from User State Migration Toolkit 4.0, which is executed in an operating system deployment task sequence. This site role is available only in the site.

System Health Validator Point When implementing Network Access Protection (NAP) a system health validator point validates the Configuration Manager NAP policies. The role needs to be installed on the NAP health policy server. This site role is available hierarchy wide.

Windows Intune Connector When managing mobile devices via Windows Intune you need to install the Windows Intune connector to be able to retrieve status messages and inventory messages from the mobile devices that are enrolled in Windows Intune.

Best Practices for Site System Design

When planning and designing a Configuration Manager 2012 site hierarchy, you also need to place your site system roles on the right server. Depending on the role and the size of the site, the role can consist of other roles on one or more site servers. This section will provide information about some best practices for capacity planning of Configuration Manager 2012.

Capacity Planning of Configuration Manager 2012

Table 2.15 lists the maximum recommendations for planning and designing your Configuration Manager 2012 infrastructure. The actual figures depend on your available hardware, your network infrastructure, and also on your demands.

TABLE 2.15: Site system planning figures

SITE SYSTEM	NUMBER	DESCRIPTION
Clients	400,000	This is the maximum number of clients supported for the entire Configuration Manager 2012 hierarchy.
Primary site	25	A Central Administration Site supports up to 25 child primary sites.
Primary site	100,000	A primary site supports up to 100,000 clients.
Secondary site	250	There is a maximum of 250 secondary sites per primary site.
Secondary site	5,000	A secondary site can support communications from up to 5,000 clients.
Management point	10	A primary site can support up to 10 management points.
Management point	25,000	One management point can support up to 25,000 clients.
Distribution point	4,000	A distribution point is capable of supporting up to 4,000 clients.
Distribution point	250	A site can hold up to 250 distribution points.
Pull distribution point	2,000	Each primary and secondary site supports up to 2,000 pull distribution points.
PXE-enabled distribution points	250	Up to 250 PXE-enabled distribution points are supported per primary site.
Software update point	25,000	If the software update point runs on the WSUS server and other site roles coexist, the software update point supports up to 25,000 clients.
Software update point	100,000	If the software update point runs on the WSUS server and no other site roles coexist, the software update point supports up to 100,000 clients.
System health validator point	100,000	The system health validator point in Configuration Manager 2012 supports up to 100,000 clients or one per hierarchy if fewer than 100,000 clients.
Fallback status point	100,000	The fallback status point in Configuration Manager 2012 supports up to 100,000 clients or one per site.
Application Catalog website point	400,000	One Application Catalog website point supports up to 400,000 clients, but for better performance, plan for 50,000 clients per point.

Site System	Number	Description
Application Catalog web service point	400,000	One Application Catalog web service point supports up to 400,000 clients. Best practice is to place the website point and web service point on the same server.
Packages and applications per distribution point	10,000	Per distribution point supports up to 10,000 packages and applications.

High Availability/Load Balancing

If there is a need for a highly available Configuration Manager 2012 infrastructure in your environment or you want to load balance some site system roles, there are some options that you can implement. The following high-availability options are offered:

Adding Extra Management Points When you add extra management points, you are providing load balancing for the management points but also a form of high availability. When one management point fails, the second management point will take over and provide connectivity.

Adding Extra Distribution Points When you add extra distribution points, you are providing load balancing for the distribution points but also a form of high availability. When one distribution point fails, the second distribution point will take over and provide access to the content.

Adding Extra SMS Providers When you add extra SMS providers, when one SMS provider is unavailable the Configuration Manager 2012 console can still access the Configuration Manager database.

Clustering Configuration Manager 2012 Database Per site you can place your Configuration Manager 2012 database on a Windows 2008 R2 or higher failover cluster.

When you place site system roles such as software update points or distribution points on dedicated servers, you spread the risks and load of the site system servers.

SQL Considerations

While planning the Configuration Manager 2012 infrastructure you also need to plan the SQL environment. The planning figures in Table 2.16 are valid for your SQL environment.

Table 2.16: Site system planning figures

Edition	Number	Description
Standard	50,000	The standard edition of SQL supports up to 50,000 clients in the hierarchy when it is collocated with a CAS server or remote from the site server.
Standard	50,000	The standard edition of SQL supports up to 50,000 clients in the site when it is collocated with a primary site server.
Standard	100,000	The standard edition of SQL supports up to 100,000 clients in the site when it remote from the site server.
Enterprise	400,000	The enterprise edition of SQL supports up to 400,000 clients in the hierarchy when it is collocated with the CAS server.

Consider the following design rules for you SQL environment:

- If you use a remote database server, ensure that the network between the site server and the remote database server is a high-available and high-bandwidth network connection.
- Each SMS provider computer that connects to the site database increases network bandwidth requirements. The exact bandwidth is unpredictable because of the many different site and client configurations.
- SQL Server must be located in a domain that has a two-way trust with the site server and each SMS provider. Best practice is to place SQL Server in the same domain as the SMS provider and SMS site servers.
- Clustered SQL Server configurations for the site database server when the site database is collocated with the site server are not supported.

Site Communications

The method of replicating data between sites has changed in Configuration Manager 2012. Synchronization of site information between sites is done by database replication, based on SQL Server Service Broker. The Data Replication Service is used to replicate the Configuration Manager 2012 database between the SQL Server databases of other sites in a Configuration Manager 2012 hierarchy. Global data and site data are replicated by database replication.

When you install a new site in the hierarchy, a snapshot of the parent site database is taken. The snapshot is transferred by server message blocks (SMB) to the new site, where it is inserted into the local database by bulk copy procedure (BCP).

For application or package content, file-based replication is still used, and it uses addresses and senders to transfer data between the sites in the hierarchy. The SMB protocol (TCP/IP port 445) is still used for file-based replication.

Table 2.17 lists the changes regarding the replication of Configuration Manager data.

TABLE 2.17: Site replication of Configuration Manager 2012 data

DATA	EXAMPLES	REPLICATION TYPE	DATA LOCATION
Global data	Collection rules, package metadata, software update metadata, deployments—anything created by administrators or scripts	SQL	Central Administration Site, all primary sites, subsets on secondary sites
Site data	Collection membership, inventory, alert messages—any data created by clients in normal operations	SQL	Central Administration Site and originating primary site
Content	Software package installation sources, software update sources, boot images	File based	Primary sites, secondary sites, and distribution points

Site Security Mode

Configuration Manager 2007 had two security modes: mixed mode and Native mode. In Configuration Manager 2007, mixed mode was the default mode, which used port 80 to communicate with the clients. Configuration Manager 2007 in Native mode was the more secure mode, which integrated PKI to secure client/server communications. The security mode in Configuration Manager 2007 was site wide.

In Configuration Manager 2012, the concept of Native and mixed modes has been replaced and simplified. You are now able to decide per individual site system role whether clients can connect through HTTP or HTTPS. Instead of configuring a site as mixed or Native mode, you must configure the site role to use HTTP (port 80), HTTPS (port 443), or both. This way, you are more flexible if you want to implement a PKI to secure intranet client communications.

To allow secure communications between your clients and site servers, a PKI needs to be present in your environment, and certificate templates need to be created to be able to enroll certificates for the Configuration Manager 2012 site systems and the Configuration Manager 2012 clients. The following site roles can be configured in HTTP or HTTPS mode:

- Management point
- Distribution point
- Enrollment point
- Enrollment proxy point
- Out of band service point
- Application Catalog web service point
- Application Catalog website point
- Software update point (SSL)

Internet-based clients and mobile devices always use secure HTTPS connections. For Internet-based clients, you need to install a site system server in a demilitarized zone (DMZ) and configure the Internet-facing site roles to accept HTTPS client communications and connections from the Internet. When you configure Configuration Manager 2012 to be accessible from the Internet, you can support your clients from the Internet. If you have a lot of mobile workers, managing your Configuration Manager 2012 clients is essential. Mobile devices communicate over the air via the Internet to your Configuration Manager 2012 environment. For this reason, the communication between the Configuration Manager 2012 environment and mobile devices must be secure.

Discovery of Your Resources

The methods of resource discovery have not changed since Configuration Manager 2007. You can use multiple ways to discover different types of resources in the network. You define which resources you want to discover, how often, and using which scope. The following methods are available:

Heartbeat Discovery Used to send a discovery data record from the client to the site periodically; it's a method to renew client data in the Configuration Manager database. Heartbeat discovery is available for primary sites.

Active Directory Forest Discovery Used to discover Active Directory forests from the Active Directory Domain Services. It discovers site server forests plus any trusted forests and supports boundary creation on demand and automatically. Active Directory forest discovery can be configured only on a CAS or a primary site.

Active Directory Group Discovery Used to discover group membership of computers and users from the Active Directory Domain Services. Active Directory group discovery is available for primary sites.

Active Directory System Discovery Used to discover computer accounts from the Active Directory Domain Services. Active Directory system discovery is available for primary sites.

Active Directory User Discovery Used to discover user accounts from the Active Directory Domain Services. Active Directory user discovery is available for primary sites.

Network Discovery Used to discover resources on the network such as subnets, SNMP-enabled devices, and DHCP clients. Network discovery is available for primary sites and secondary sites.

Be sure to plan the resource discovery well. For instance, if there is no need to discover the whole Active Directory, plan the resource discovery to discover only resources in dedicated Active Directory organizational units. This way you keep the Configuration Manager environment free of unwanted objects. Discovered resources can be added to collections, which can be used to deploy applications or compliancy settings to the resources, for example. You will find more information about discovering your resources in Chapter 6, "Client Installation."

Client Settings and Client Deployment

With Configuration Manager you are able to create different client user and client device settings packages for different collections. Besides the default client agent settings that are available for the entire hierarchy, you can create custom client settings that you can assign to collections. Custom client settings override the default client settings. The resultant settings can be an aggregation of default and one or more custom settings.

Implementing client settings is the easiest step to reduce the infrastructure; there is no need for primary sites for different client settings.

Depending on the implementation or migration scenario, different ways of deploying the Configuration Manager client to the devices are supported. Configuration Manager 2012 still supports the client push mechanism and pushing clients via the WSUS infrastructure. Deploying the client with a third-party application deployment environment or Active Directory is of course also possible. Read more about installing Configuration Manager clients and client settings in Chapter 6.

Content Management

Managing content in Configuration Manager 2012 can be done on different levels and in different parts of the Configuration Manager 2012 console:

Distribution Points/Distribution Point Groups Per distribution point or distribution point group you are able to see, redistribute, validate, or remove content easily. Content validation can be done automatically based on a schedule. When adding a new distribution point to a distribution point group, all the applications or packages assigned to a distribution point group will be automatically copied to the new distribution point.

Content-Related Objects Objects that have content have a Content Locations tab where you can manage the content and see on which distribution point the content is available. From the object you are also able to validate, redistribute, and remove the content from the distribution points. Objects that have content are applications, packages, boot images, driver packages, operating system images, operating system installers, and software update deployment packages.

Monitoring In the monitoring workspace of the Configuration Manager console you can monitor your applications and packages in the Content Status node. You can also monitor the distribution point group status and distribution point configuration status.

Role-Based Administration

In Configuration Manager 2012, role-based administration is a feature that brings you "Show me what's relevant for me" based on security roles and scopes. Configuration Manager 2012 comes with 15 standard roles, and you can also create custom roles.

Role-based administration is based on the following concepts:

Security Roles What types of objects can someone see, and what can they do to them?

Security Scope Which instances can someone see and interact with?

Collections Which resources can someone interact with?

As part of role-based administration you are able to limit collections; every collection is limited by another. Assigning a collection to an administrator will automatically assign all limited collections.

While planning role-based administration, explore the 15 standard roles and assign the rights to your administrators depending on the part of Configuration Manager they need to manage.

The 15 different roles from which you can choose are these:

- Application administrator
- Application author
- Application deployment manager
- Asset manager
- Company resource access manager
- Compliance settings manager
- Endpoint protection manager
- Full administrator
- Infrastructure administrator
- Operating system deployment manager
- Operations administrator
- Read-only analyst
- Remote tools operator
- Security administrator
- Software updates manager

Role-based administration allows you to map organizational roles of administrators to security roles. Hierarchy-wide security management is done from a single management console.

You can add Active Directory user accounts to Configuration Manager 2012 in the Configuration Manager 2012 console. In the Administration workspace you will find Administrative Users under Security; here you can add the user accounts from your users who need to have access to Configuration Manager 2012. After adding the user accounts you can assign them the proper role.

Migration

In Configuration Manager 2012 the migration feature is used to migrate your Configuration Manager 2007 investments or investments made in another Configuration Manager 2012 environment to the new user-centric platform. With the migration feature you can migrate the following objects:

- Collections (from Configuration Manager 2012 only)
- Deployments (from Configuration Manager 2012 only)
- Software distribution deployments
- Task sequence deployments
- Application deployments
- Software update deployments
- Software update list deployments
- Baseline deployments
- Boundaries
- Boundary groups (from Configuration Manager 2012 only)
- Global conditions (from Configuration Manager 2012 only)
- Software distribution packages
- Applications (from Configuration Manager 2012 only)
- Virtual application packages (from Configuration Manager 2007 only)
- App-V virtual environments (from Configuration Manager 2012 only)
- Software updates
- Deployments
- Deployment packages
- Deployment templates
- Software update lists
- Software update groups (from Configuration Manager 2012 only)

- Automatic deployment rules (from Configuration Manager 2012 only)
- Operating system deployment
- Boot images
- Driver packages
- Drivers
- Images
- Installer
- Task sequences
- Settings management
- Configuration baselines
- Configuration items
- Asset Intelligence
- Catalog
- Hardware requirements
- User-defined categorization list
- Software metering rules
- Saved searches (from Configuration Manager 2012 only)

How Can You Prepare Your Configuration Manager 2007 Environment?

Before planning for a migration of your Configuration Manager 2007 environment, prepare the environment so it is compliant on the following matters:

- Flatten your hierarchy where possible, for instance, by removing secondary sites or unnecessary primary sites in the Configuration Manager hierarchy.
- Plan for Windows Server 2008 R2, SQL 2008, and 64-bit by acquiring hardware that is compatible with 64-bit software.
- Start with the implementation of BranchCache with Configuration Manager 2007.
- Move from web reporting to SQL Reporting Services by configuring the reporting site role in Configuration Manager 2007.
- Avoid mixing user and device-collection definitions.
- Use UNC paths in your packages instead of local paths.

Migrate your Windows XP branch distribution points to Windows 7.

Be sure to always plan your migration, and address the following subjects in your migration plan:

- Prepare the Configuration Manager 2007 environment to be able to migrate the objects to Configuration Manager 2012.
- Decide how often the data-gathering process needs to be run.
- Determine which objects you are going to migrate.
- Discover where the objects are that need to be migrated.
- Determine how to migrate the distribution point and whether you will use distribution point sharing.
- Plan the client migration.
- Decide how to remove the Configuration Manager 2007 environment.

You can read more about the migration feature in Chapter 3, "Migrating to Configuration Manager 2012."

Disaster Recovery

When planning a new Configuration Manager 2012 infrastructure, be sure to also make a disaster recovery plan. Since Configuration Manager 2012 is an important part of your IT infrastructure, you will need to be sure that when a disaster occurs, your Configuration Manager 2012 infrastructure will not be affected.

To protect yourself from failure, you can make your environment highly available. This can be done by implementing the following options:

- Installing more than one primary site server in a site
- Placing the Configuration Manager databases on a SQL cluster
- Installing more than one site role per site

It is recommended that you test your disaster recovery plan in a test environment so you can document the disaster recovery process and know what to expect while recovering your Configuration Manager 2012 environment.

You can read more about disaster recovery in Chapter 18, "Disaster Recovery."

Designing Your Configuration Manager Environment

After you've gathered your information about the new Configuration Manager 2012 infrastructure, you can design the new infrastructure. When designing a new Configuration Manager 2012 infrastructure, you need to keep a couple things in mind. Whereas in SMS 2003 and Configuration Manager 2007 you could easily design an infrastructure based on bandwidth, languages, or administrative purposes, in Configuration Manager 2012 the hierarchy is simplified and modernized. For most cases you can do more with less. Of course, you still need to identify your network locations and the bandwidth between your locations. Keep in mind that Configuration Manager 2012 has the goal of simplifying your Configuration Manager infrastructure by flattening the hierarchy and by server consolidation.

Noncritical Design Issues

The design of Configuration Manager 2012 was changed; for this reason, the following items are no longer critical decision points for designing a site hierarchy:

- Support of multiple languages
- Different client settings per region
- Decentralized administration of your Configuration Manager infrastructure
- Logical data segmentation
- Content routing for deep hierarchies

When designing a Configuration Manager 2012 infrastructure, you will need to review your gathered intelligence and translate this into a design. Things you need to take in account are the following:

Physical Locations of Your Environment As we said, the first step is to translate your network infrastructure information into information that can be used for the design of the Configuration Manager infrastructure. Ask yourself the following questions:

- Where are my locations?

  Are my locations in the same country? If so, larger locations often are well-connected sites, and smaller locations usually have less bandwidth available.

- Are my locations on the same continent?

  If your locations are on the same continent, you need to place a management point at your site, and you can create a secondary site for each location. If a location is not on the same continent, it is wise to create a primary site for that location.

- What is the available bandwidth?

  For well-connected locations it is often unnecessary to create a Configuration Manager site for that location. If there is a need for local content, you can install a distribution point on such locations since the distribution point now has throttling and bandwidth control.

- How many users are working at the location?

  One primary site can handle 100,000 clients. Depending on your hardware performance and bandwidth, you can implement one primary site for your entire Configuration Manager infrastructure. Consider using BranchCache for small locations or just a distribution point.

- What kind of traffic needs to flow down in the network?

  Depending on the data that needs to flow down for administrative or political reasons, it might be necessary to implement a primary site at a location that should normally not be a primary site because of the size or available bandwidth.

Central Administration Site or Not? When you need more than one primary site in your Configuration Manager infrastructure, you also need a Central Administration Site. The placement of this CAS can be a design choice, but often you will place this site at the datacenter or the location where the IT department resides. Configuration Manager clients do not connect to a CAS.

High Availability Considerations If you need a highly available Configuration Manager site or infrastructure, you can install multiple roles (management point, provider, and so on) of the same role in one site without the need for network load balancing. The Configuration Manager 2012 client automatically finds the right management point if one is offline. You also can cluster the SQL database.

Client Settings As we said, client settings are no longer a reason to implement a primary site. Multiple client settings can be assigned to collections of users or computers. While designing, try to define different client settings for the groups of users or computers as needed. Otherwise, just use the default client settings.

Boundary Management Boundaries and boundary groups are fundamentals of your Configuration Manager infrastructure. Be sure to identify all the boundaries so that all the Configuration Manager clients can be managed.

Virtualization Microsoft supports the virtualization of Configuration Manager site servers. Before implementing, always check the Microsoft website for the latest versions and supported third-party virtualization software.

Managing Untrusted Environments In the past you could manage untrusted domains by supplying accounts with rights. With Configuration Manager 2012 you can manage other forests only via two-way trusts.

Another way is to install site roles in an untrusted domain, but it cannot be a primary site role. You can provide some services but not all of them.

Naming the Configuration Manager Sites After determining your sites in your Configuration Manager 2012 infrastructure, you need to name the Configuration Manager sites. Like in earlier versions, you use a three-character-length code. The site code can contain only standard characters (A–Z, a–z, 0–9, and the hyphen, "-") and must be unique for your Configuration Manager infrastructure. In earlier versions of Configuration Manager you were not able to use Microsoft reserved names: SMS, CON, PRN, AUX, NUL, OSD, SRS, or FCS. This is still the case.

Planning the Configuration Manager Hierarchy

When designing your Configuration Manager hierarchy you need to create an implementation plan for where to install which server with what kind of roles. The deployment information you gathered in an earlier stage will provide the requirements for where you need to install the Central Administration Site, primary sites, secondary sites, and distribution points. To come up with the right design, follow these design steps:

1. Define a naming convention if one doesn't already exist.
2. Determine whether a CAS is needed and where to place this site in your environment. The CAS is the topmost site in your Configuration Manager hierarchy.
3. Define the placement of the primary sites, secondary sites, or just distribution points; remember that tiering primary sites is no longer possible. Look at your WAN and keep the design rules in mind and which roles you need in a specific site.

4. Look at the logical and physical connections between your Configuration Manager sites so you can decide whether addresses need to be configured to manage the traffic between the sites.
5. Assign the boundaries that represent your Configuration Manager sites, and be sure that no boundaries overlap each other.
6. Depending on the Configuration Manager sites, high-availability demands, and other requirements, you can place the site system roles where they are needed.

Designing a good Configuration Manager hierarchy is a must for an effective and solid Configuration Manager infrastructure. Always check the proposed design, and if possible let someone else review the design.

Planning Configuration Manager Site Systems

After designing and planning the Configuration Manager hierarchy, the next step is to plan and design your site systems. This is done by analyzing your requirements per site, gathered during the deployment intelligence phase, described in the section "Gathering Deployment Intelligence." Depending on the expected load and the number of connecting users, you can place roles on different servers or group them on one server.

When planning a highly available Configuration Manager infrastructure, you will need to plan several site roles on more than one server. Not all roles can be installed on every site, so be sure that you determine this while planning the hierarchy.

For detailed information on all the Configuration Manager 2012 site system roles and the installation of these roles, see Chapter 4.

Planning Configuration Manager Clients

The clients managed by Configuration Manager 2012 are an essential part of the Configuration Manager infrastructure. You need to plan the deployment of your Configuration Manager 2012 clients while migrating from Configuration Manager 2007 or while building a new Configuration Manager 2012 because the deployment can be carried out in different ways. Planning your Configuration Manager 2012 client agent settings is also essential. In Configuration Manager 2012 you can create more than one client settings package.

Client Installation Planning

Like in earlier versions, you are able to deploy the Configuration Manager 2012 client via different methods. Depending on your scenario, you can choose different ways to deploy the Configuration Manager client to clients:

- When clients are managed by a third-party desktop management tool, you can choose to install the client via the current desktop management tool or install it via the supported ways in Configuration Manager 2012, via client push and software updates. Or you can choose to deploy a new operating system to the clients with the operating system deployment feature of Configuration Manager.
- When clients are managed with Configuration Manager 2007, you can migrate the clients to the new Configuration Manager 2012 management point.
- Unmanaged clients can receive a client via the supported ways in Configuration Manager 2012, via client push and software updates. Or you can choose to deploy a new operating system to the clients with the operating system deployment feature of Configuration Manager.

Every solution has it pros and cons, but try to find out which method is the best for your environment. For instance, installing a Configuration Manager client on an unmanaged client can result in lots of legacy and unmanaged software in your environment. Installing a new operating system on thousands of clients can be a lot of work and very expensive.

You can read more about client installation methods and best practices in Chapter 6.

Client Agent Planning

A Configuration Manager client consists of agents that support several Configuration Manager features. There is one default Client Settings package with settings for all manageable agents. With Configuration Manager 2012 you are able to create custom client settings and deploy them to clients on collection levels to users or devices.

Planning your client (agent) settings is more complex, because you have the ability to assign client settings to collections. For this reason it's important to analyze the needs of groups of devices and the users. You can read more about client settings methods and best practices in Chapter 6.

Determining How to Deploy Configuration Manager

After you have verified your site design in your test lab, you should plan an initial pilot deployment of Configuration Manager on a small section of your network. Monitor the deployment progress and any potential client problems with your first-level support department.

With the lessons that you learn during your pilot deployment, you'll be able to decide which method of Configuration Manager installation to use for your site deployment. Your goal will be to accomplish the deployment as efficiently as possible while preserving the functionality of any previous methods of system management that you already have in place for as long as needed. The deployment method you use will then help you decide whether you will need additional hardware or personnel resources to do that.

There are several starting points for an implementation of the new Configuration Manager 2012 infrastructure. When a Configuration Manager 2007 infrastructure is already in place, you will probably choose to migrate the environment via the side-by-side migration feature, which is available in Configuration Manager 2012. If you have a version older than Configuration Manager 2007, then you have only two options since direct migration of earlier versions is not supported:

- Build a *greenfield* (new) Configuration Manager 2012 infrastructure.
- Migrate first to Configuration Manager 2007 and then perform a side-by-side migration.

If you don't have any Configuration Manager infrastructure in place, you need of course to build a new environment without migrating any assets. An in-place upgrade like that supported in earlier versions is not supported by Configuration Manager 2012.

In the next chapter you will read more about the migration options and the dos and the don'ts when migrating assets from Configuration Manager 2007.

Building a Proof-of-Concept Environment

After your plan and design phase is finished, you need to verify your design in a test or *proof-of-concept* (POC) environment. In this environment you can test your future Configuration Manager 2012 environment and create, if necessary, a detailed migration plan. The POC environment can also be used to train your Configuration Manager administrators so that they become familiar with the new environment and will accept the new Configuration Manager 2012 environment.

Be sure to create a test plan upfront as a guideline for your proof-of-concept phase of the project. A few test steps that you want to take are shown here; depending on your demands, you can shorten or lengthen the list:

- Deployment of the Configuration Manager 2012 clients
- Deployment of applications, software updates, and settings
- Deployment of operating systems
- Synchronization of data between sites
- Migration of objects from Configuration Manager 2007

If all tests are successful, you can start implementing the new Configuration Manager 2012 infrastructure in the production environment. Be sure to keep the POC environment so that you will have a test lab for testing future changes in the Configuration Manager 2012 environment or for testing your disaster-recovery plan.



Real World Scenario

Implementing a New Configuration Manager Infrastructure

Sports Clothes United Inc. develops and sells sportswear to retailers and their own shops all over the world. The head office is located in San Francisco. The company is growing fast, and they are now using a third-party deployment tool for applications and operating systems.

You as a consultant or Configuration Manager administrator are asked to develop a real desktop management environment where user experience is the key to the success of the project and acceptance.

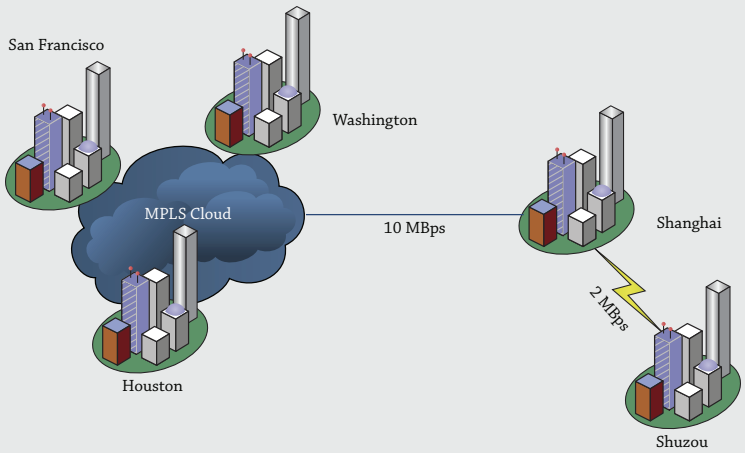
Deployment Intelligence

As we said, Sports Clothes United is using a third-party deployment tool, and the assets and investments made in the years they were not using it are not compatible for migration. The company has four locations with offices and factories spread over the United States and China, and they are planning to open offices in Europe soon. The proposed Configuration Manager environment must be scalable and support future expansions.

Currently Sports Clothes United has major offices and factories in San Francisco, Houston, Shanghai, and Suzhou. The corporate systems are available from a datacenter in Washington, D.C. The local stores in the United States connect through an MPLS network to the nearest office. In China the offices and plants are connected through a 2-MB fiber connection. The United States and China are connected through a 10-MB fiber connection.

The following locations serve local or remote clients:

- Washington, D.C.: no clients connecting
- Houston: 1,000 clients connecting
- Shanghai: 3,000 clients connecting
- Suzhou: 100 clients connecting



At this time Sports Clothes United isn't able to support their users at the level they want. The corporate IT department is professionalizing their processes, and they currently cannot service their internal customers according to the service-level agreement. To be able to do this they want to have the following features in their new Configuration Manager 2012 infrastructure:

- Software inventory
- Hardware inventory
- Software distribution to any (mobile) workplaces
- Zero-Touch operating system deployment of Windows 7 Multi-Language
- Wake On LAN
- User self-service portal to request or install applications
- Deployment of software updates
- Compliancy settings management to control the workplace
- Role-based administration for delegation of tasks
- Software metering to control licenses
- Remote administration to support internal customers
- Support for mobile device management

For software updates in the United States, a local software update point must be present in every major location.

One of the major requirements in managing applications is that the new environment must support people bringing their own devices to work. Supporting this new way of working is the key to success because it will promote internal customer satisfaction. The assets owned by Sports Clothes United must be able to receive a corporate image, and applications installed via Microsoft Installer Package (MSI) and assets that are brought in or are owned by the employees must be able to receive a virtualized version of that same application. Support for Virtual Desktop Infrastructure (VDI)- and Server Based Computing (SCB)-based environments is also a must-have.

Deployment Planning

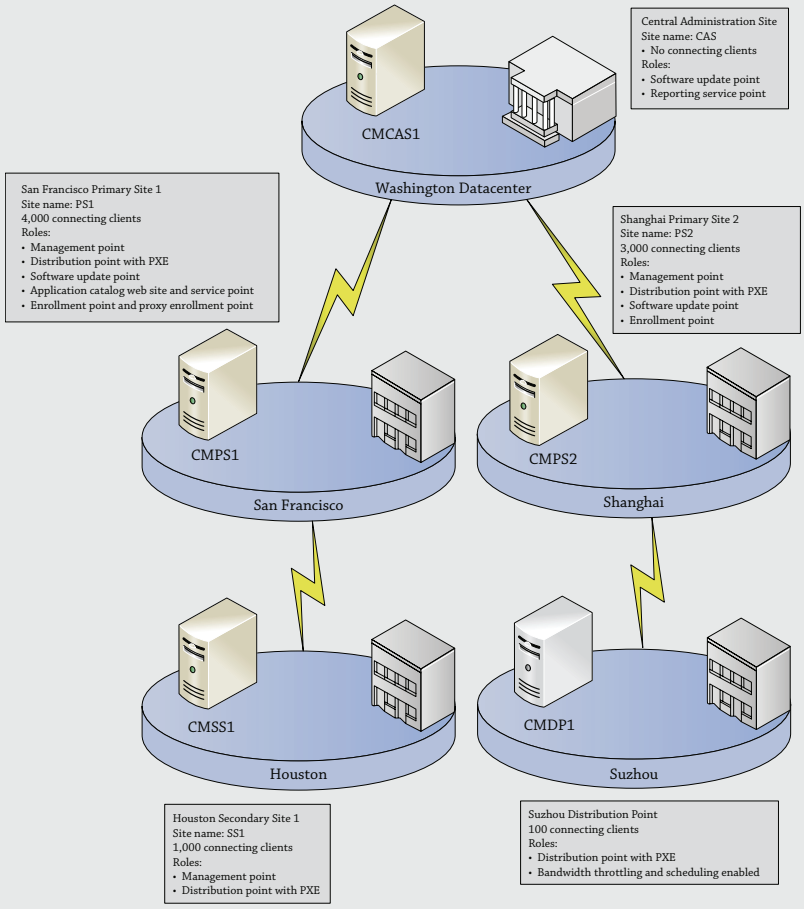
With the information and requirements gathered during the deployment intelligence phase of your project, you now need to translate the information requirements to a design and a deployment plan.

One of the best practices is not to create a primary site that covers more than one continent. Since Sports Clothes United currently has locations in two continents and is planning one or more in Europe, you will need to place a primary site in North America and one in Asia.

Because of the fact that the company needs two or more primary sites, a Central Administration Site is needed. The datacenter in Washington, D.C. can be used for the CAS. No clients will connect to this site.

The locations in San Francisco and Shanghai are chosen as primary sites because of the size of the location in Shanghai and the availability of the corporate IT in San Francisco. The Houston site will be a secondary site because of the requirement that all sites in the United States need a local software update point. The site in Suzhou will receive a local distribution point with PXE, bandwidth control, and throttling enabled and configured.

The basic proposed Configuration Manager hierarchy is shown here.



This Configuration Manager 2012 infrastructure can be a greenfield environment, and the transition will be done after a pilot phase has proven that the requirements have been met.

The Bottom Line

Plan and design a Central Administration Site. One of the first questions you will ask yourself while starting to design and plan a new Configuration Manager 2012 hierarchy is "Do I need a Central Administration Site?" The answer to this question is essential for your final design.

Master It Determine when a CAS is needed.

Plan and design an effective Configuration Manager 2012 infrastructure. When planning and designing a new Configuration Manager 2012 infrastructure, it is important to plan your site placement appropriately. The design rules for primary sites have changed from how they were in Configuration Manager 2007.

Master It Understand the reasons for not needing an additional primary site implementation.

Identify the enhancements to the distribution point site system role. Distribution points in older versions were used to provide local points for accessing content and later also for App-V streaming. In Configuration Manager 2012 distribution points do a lot more.

Master It Distribution points have been enhanced. What roles and components are merged with the new distribution point, and what's new?

Prepare your current Configuration Manager 2007 environment for migration to Configuration Manager 2012 An in-place upgrade of Configuration Manager 2007 to Configuration Manager 2012 is not supported. Configuration Manager 2012 has a migration feature within the feature set to enable side-by-side migration.

Master It How can you as a Configuration Manager administrator or consultant prepare a current Configuration Manager 2007 environment for migration to Configuration Manager 2012?



Chapter 3

Migrating to Configuration Manager 2012

In the past, an upgrade or migration of Systems Management Server (SMS) to Configuration Manager 2007 was not an easy process. You could migrate the SMS 2003 environment side-by-side manually or by using scripts, but at the end of the process you were not able to monitor the migration of your objects. Very often a *greenfield* (new) environment was created next to the old SMS infrastructure, and the objects that were needed in the new Configuration Manager 2007 infrastructure had to be re-created by hand.

For Configuration Manager 2012, Microsoft invested a lot of time in creating a good, solid migration scenario that is easily managed. The new feature, called *migration*, allows you to migrate your objects to the new Configuration Manager 2012 infrastructure. In addition, since Configuration Manager SP1, you can migrate objects not only from a Configuration Manager 2007 site but also from a source Configuration Manager 2012 R2 hierarchy.

The migration feature in Configuration Manager 2012 will assist you with the following goals:

- Migrating Configuration Manager 2007 objects
- Migrating Configuration Manager 2007 clients
- Migrating Configuration Manager 2012 (R2) objects
- Migrating Configuration Manager 2012 (R2) clients
- Minimizing WAN impact
- Flattening the Configuration Manager infrastructure by reducing the number of primary sites
- Maximizing the reusability of 64-bit–capable hardware

Besides the migration feature, you can wipe and load your Configuration Manager environment while, for instance, you are still using SMS 2003.

In this chapter, you will learn to

- Determine what you are able to migrate with the migration feature
- Discover which migration approach is supported
- Ascertain what kind of interoperability is supported during the migration
- Migrate packages and programs to the new application model

Introducing Migration

The migration feature and the migration concept bring with them some new terminology. In this section you will find out what's covered in the migration feature and where you can find it in Configuration Manager 2012.

Client Information Client information includes such items as the client globally unique identifier (GUID), the inventory, and the client status information. Every Configuration Manager 2012 client has an ID that is unique in the Configuration Manager 2012 environment.

Client Migration The process of upgrading the Configuration Manager client of the source hierarchy to the new Configuration Manager 2012 hierarchy is called *client migration*. This process can be initiated in different ways, but during the migration process the old Configuration Manager client will be uninstalled and the new Configuration Manager 2012 client will be installed.

Content The content consists of the package binaries and files. The source of these packages needs to be accessed via a UNC path. The UNC path must be available for the Configuration Manager 2012 site server.

Data Gathering One of the first steps in the migration process is that the Configuration Manager 2012 R2 hierarchy discovers all the objects in the source Configuration Manager environment. The source Configuration Manager environment can be based on the versions Configuration Manager 2007 and 2012. To be able to discover the objects, you need to configure a data-gathering process that is part of the migration feature.

This data gathering is an ongoing migration process that discovers all the objects or changes in the old infrastructure. During the migration period, this process is scheduled by default to run every four hours.

Migration Jobs Migration jobs are used to migrate specific objects from the source Configuration Manager hierarchy to the new infrastructure. Migration jobs can be scheduled for the future or started instantly.

Monitoring Migration While migrating assets from the source Configuration Manager to the target Configuration Manager, it is useful to be able to monitor the migration process. Monitoring your migrations can be done from the Configuration Manager 2012 console, specifically in the Administration workspace under Migration ➢ Migration Jobs. You will be able to see which migrations completed, which failed, and which are in progress or need to be completed.

Objects Objects subject to migration include packages, applications, software update deployments, driver packages, OS images, configuration items, and the like within Configuration Manager.

Server Settings Server settings are the site role settings and site properties in the Configuration Manager hierarchy.

Shared Distribution Points Shared distribution points are distribution points that are active in the source Configuration Manager hierarchy. Enabling shared distribution points allows you to use the source Configuration Manager distribution points in the new Configuration Manager 2012 infrastructure. During the migration process, the Configuration Manager 2012 clients can receive the content from the shared distribution points. The shared distribution points are read only though; they are still managed by the source Configuration Manager hierarchy. After the shared distribution points are reassigned to the target hierarchy, they will be manageable by this Configuration Manager hierarchy.

Source Hierarchy The source hierarchy is the Configuration Manager 2007 or Configuration Manager 2012 R2 hierarchy from which you want to migrate objects to the Configuration Manager 2012 R2 infrastructure. The source hierarchy is always the topmost site of the source Configuration Manager hierarchy.

Source Sites Source sites are the sites in the source hierarchy that hold Configuration Manager data that you want to migrate to the target Configuration Manager site. You need to configure account settings per source site to be able to connect to each source site.

Migration Functionality in Configuration Manager 2012

Configuration Manager 2012 comes with a migration feature that allows you to migrate your objects from a source Configuration Manager site to a target Configuration Manager site. Migrating objects is done via migration jobs, but first you need to designate a source hierarchy to be able to gather information from the source hierarchy and to create migration jobs.

Source Hierarchy

When migrating a Configuration Manager 2007 or 2012 hierarchy to a new Configuration Manager 2012 R2 hierarchy, you need to specify a source hierarchy. You must use the topmost Configuration Manager primary site server as the source hierarchy, as shown in Figure 3.1.

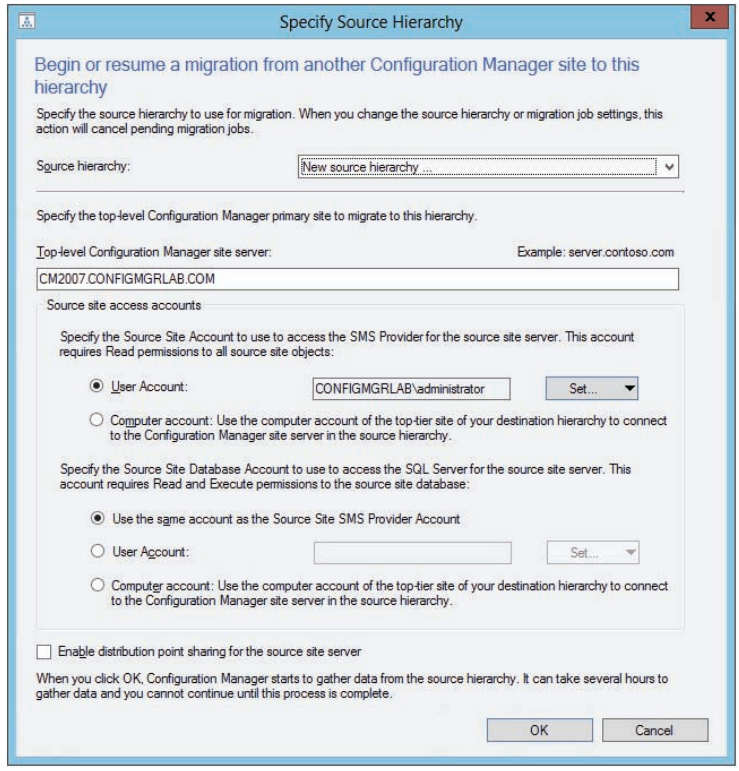


Figure 3.1 Specifying the Configuration Manager source hierarchy

During the creation process you need to supply a user account that has access to the SMS provider of the source site. This account needs read permission to all the objects in the source site—be sure to test the connection and the permissions. For SQL access you can use the same account, you can specify a different user, or you can use the local system account of the Configuration Manager 2012 central administration site or stand-alone site to connect to the source Configuration Manager site database. The user account needs read and execute permissions.

After you specify the source hierarchy, the data-gathering process may take several hours depending on how many objects are found in the source hierarchy.

Once the data-gathering process has finished discovering, it may have discovered other sites in the hierarchy. For those sites you will need to supply credentials with the right permissions per discovered site to be able to access the objects in the discovered sites in the hierarchy.

Data-Gathering Process

The initial data-gathering process can take a while depending on your source hierarchy. It will gather all information about the configured site, the object data, and information about other child sites in the hierarchy. It will also set up the connection between the source Configuration Manager site and the target Configuration Manager 2012 site. The data-gathering process must be complete before you can proceed with creating migration jobs or configuring credentials for other sites. Depending on the size of the source hierarchy, the data-gathering process can run from a couple of minutes to several hours. The more objects you have in the source hierarchy, the longer the data-gathering process will take.

The data-gathering process runs every 4 hours by default, but you can change this interval at the source hierarchy object to 1 hour, 2 hours, 4 hours, 8 hours, 12 hours, 18 hours, or 24 hours. The process runs periodically to keep the data accurate for the migration. The gathered information is stored in the Configuration Manager 2012 database for reporting purposes.

The data-gathering process can be stopped by using the Stop Gathering Data action on the ribbon of the Configuration Manager 2012 console. While gathering data you can check the `migmctrl.log` located in the `Logs` folder in the Configuration Manager 2012 installation path. The `Logs` folder can also be accessed via the `%SMS_LOG_PATH%` environment variable.

Migration Job Types

The migration of Configuration Manager objects from the source hierarchy is done by creating migration jobs. Configuration Manager 2012 supports three kinds of migration jobs, so you can choose how and when you want to migrate your assets. These three kinds of migration jobs are explained in the following sections.

Collection Migration

With the Collection Migration option you can migrate all the objects that are related to the collection, including all objects that are related to members of the collection. When you choose this option, you are able to exclude specific kinds of objects.

You are not able to migrate all Configuration Manager objects via the Collection Migration option since not all objects are related to collections. Collection Migration is available only when migrating from Configuration Manager 2007.

With Collection Migration, you can migrate the following related objects:

- Advertisements
- Software distribution packages
- Virtual application packages
- Software update deployments
- Software update deployment packages
- Operating system deployment boot images
- Operating system deployment images
- Operating system deployment operating system installers
- Task sequences
- Configuration baselines
- Configuration items

If you deselect one of these objects, then the object is placed in an exclusion list. The exclusion list can be managed from the administrative console and can be used as a reference when you want to migrate certain objects. Objects on the exclusion list are still available for migration in jobs that you create in the future. They will not be automatically selected when listed in the exclusion list.

Object Migration

With the object migration job type you are able to migrate individual objects or object types that you select. This way you can easily migrate your operating system deployment objects, for instance, to test your operating system deployment feature in Configuration Manager 2012.

With object migration, you can migrate the following object types:

- Collections (from Configuration Manager 2012 only)
- Deployments (from Configuration Manager 2012 only)
  - Software distribution deployments
  - Task sequence deployments
  - Application deployments
  - Software update deployments
  - Software update list deployments
  - Baseline deployments
- Boundaries
- Boundary groups (from Configuration Manager 2012 only)

- Global conditions (from Configuration Manager 2012 only)
- Software distribution packages
- Applications (from Configuration Manager 2012 only)
- Virtual application packages (from Configuration Manager 2007 only)
- App-V virtual environments (from Configuration Manager 2012 only)
- Software updates
  - Deployments
  - Deployment packages
  - Deployment templates
  - Software update lists
  - Software update groups (from Configuration Manager 2012 only)
  - Automatic deployment rules (from Configuration Manager 2012 only)
- Operating system deployment
  - Boot images
  - Driver packages
  - Drivers
  - Images
  - Installer
  - Task sequences
- Settings management
  - Configuration baselines
  - Configuration items
- Asset Intelligence
  - Catalog
  - Hardware requirements
  - User-defined categorization list
- Software metering rules
- Saved searches (from Configuration Manager 2012 only)

Objects Modified After Migration

With the Objects Modified After Migration option you can re-migrate objects from the source Configuration Manager hierarchy that have been migrated before and that have been changed

in some way at the source hierarchy. The wizard shows you only the objects that have been changed.

With the Objects Modified After Migration option, you can migrate the following object types:

- Boundaries
- Software distribution packages
- Software update deployment packages
- Software update deployment templates
- Software update lists
- Operating system deployment boot images
- Operating system deployment driver packages
- Operating system deployment drivers
- Operating system deployment images
- Operating system deployment operating system installers
- Task sequences
- Configuration baselines
- Configuration items
- Asset Intelligence Catalog
- Asset Intelligence hardware requirements
- Asset Intelligence software list
- Software metering rules

To successfully re-migrate virtual application packages, you first need to delete any virtual application packages from the target Configuration Manager 2012 infrastructure.

These objects are all described in detail in the following sections.

Collections

Collections can be migrated, but there are a couple of things that you need to take into account when migrating collections to the new Configuration Manager 2012 infrastructure.

In the new Configuration Manager infrastructure, subcollections and linked collections no longer exist. Also collections with *both* users and devices are not supported and will not be migrated to Configuration Manager 2012. In Figure 3.2 the Collections That Cannot Be Migrated dialog box shows that mixed query collections, mixed collection hierarchies, or collections limited to multiple other collections in Configuration Manager 2007 cannot be migrated.

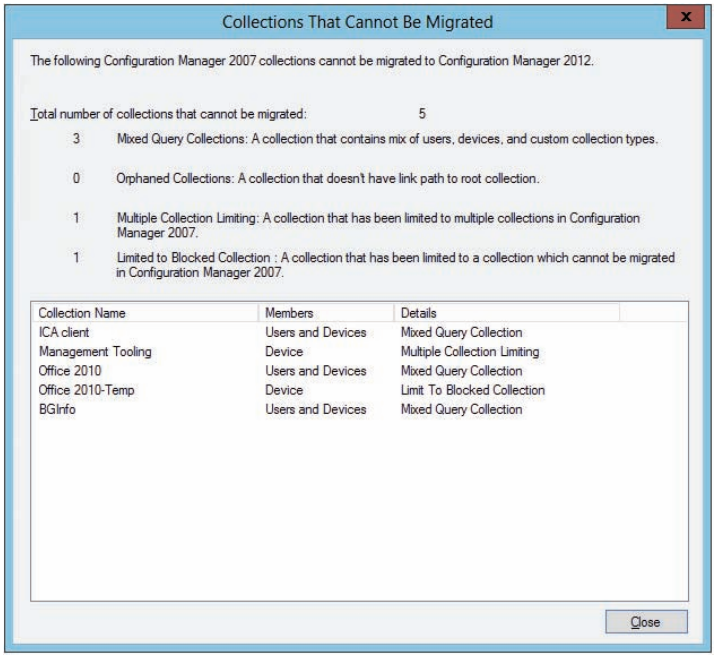


FIGURE 3.2
Collections that cannot be migrated are automatically discovered.

Some rules regarding the migration of collections apply:

- If you build a hierarchy of collections in Configuration Manager 2007, the related empty collections are migrated to folders. This way your collection organizational structure is preserved.
- Empty collections are migrated as folders (migrating only from Configuration Manager 2007).
- Direct membership collections are migrated as is and also when the direct membership is a Configuration Manager client in the source hierarchy that has not yet migrated to the new Configuration Manager 2012 site.
- Underlying collections with a mixed collection in the hierarchy cannot be migrated.
- To successfully migrate, a collection must contain either users/user groups or systems, but not both.
- Collections that are limited to multiple collections in Configuration Manager 2007 cannot be migrated.
- Collections that are limited to blocked collections in Configuration Manager cannot be migrated.

In Configuration Manager 2007 collections created in a central site were replicated down to the child sites. Collections created in a child site were replicated only within the site where the collection was created. This way the collections were limited to the child site. In Configuration Manager 2012 the collection definitions are globally replicated. The migration feature in Configuration Manager 2012 will assist you to prevent unintentionally increasing the scope of the migrated collections during the migration process. A dialog box like the one shown in Figure 3.3 will help you to limit the collection scope.

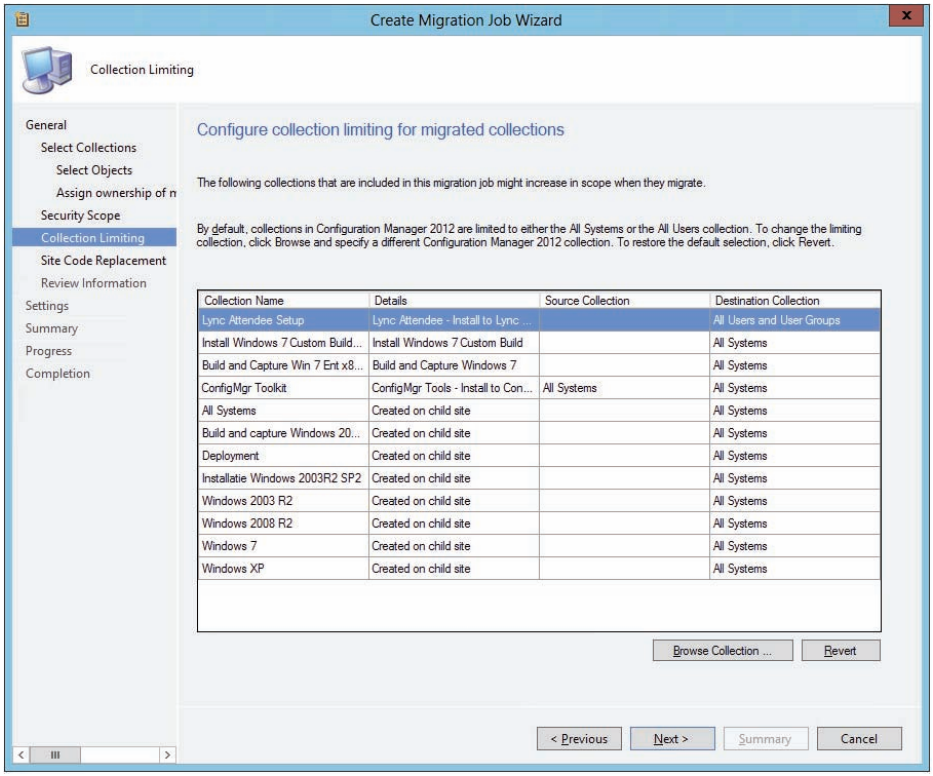


FIGURE 3.3 Limit collections for which the scope will be possibly increased.

When using site codes in collection query definitions at your source Configuration Manager hierarchy, you will be assisted in replacing the site code during the migration of the collections. It is mandatory for the new Configuration Manager 2012 hierarchy to use new site codes. In Figure 3.4 you can see that site code PS7 is replaced with PS1. With the pull-down option you can choose whatever site code you want to replace.

With the collection migration job type, you will be assisted with the migration of the collections and the migration of the related Configuration Manager objects from the source hierarchy. The feature will preserve customer investments in collections and advertisements.

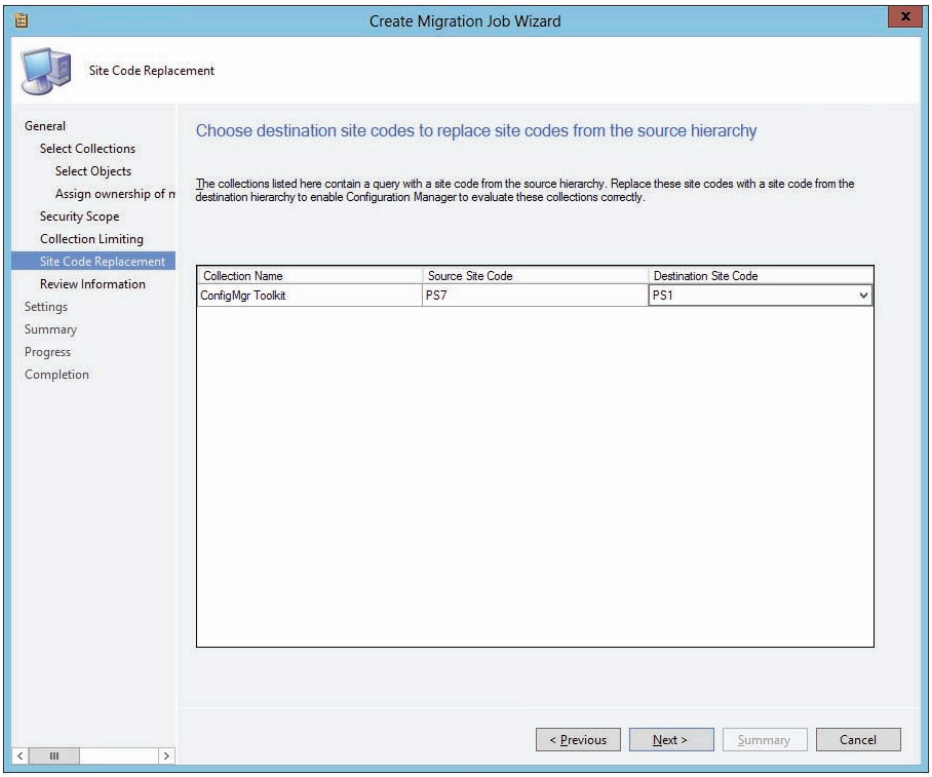


Figure 3.4
Replacing the discovered source site code with the new site code

Advertisements and Deployments

Advertisements are migrated and converted to deployments. The settings are preserved. During the collection migration job, you can automatically enable the deployment after the migration; by default the deployment is not enabled. Advertisements from Configuration Manager 2007 are migrated only if they are associated with a collection migration job and the Configuration Manager administrator has chosen to also migrate all the depended objects in addition to the collection itself. Deployments already deployed in Configuration Manager 2012 are migrated to the target Configuration Manager environment.

When an advertisement is migrated and converted, the deployment will *not* deploy the software again to computers or users where the software was already deployed in the source site. The reason for that is that the package IDs of the software packages and advertisements are preserved as part of the migration to the target Configuration Manager 2012 hierarchy. Since clients retain execution history, and it is tracked by the package ID, clients will not rerun a migrated package deployment after they have been migrated to the new hierarchy.

Boundaries and Boundary Groups

While you are migrating boundaries from Configuration Manager 2007, boundary groups are automatically created by the migration process and are enabled only for content lookup. This way you will avoid boundary overlap in Active Directory, and it will prevent new Configuration

Manager clients from getting assigned to the new Configuration Manager environment unexpectedly. When migrating from a Configuration Manager 2012 source hierarchy, you are able to migrate both the available boundaries and boundary groups.

When Distribution Point Sharing is enabled, boundaries associated with the distribution points in the source Configuration Manager hierarchy are migrated automatically.

Global Conditions

Global conditions are available only in Configuration Manager 2012. Custom global conditions that you have created are the only global conditions that are able to migrate from the source Configuration Manager 2012 hierarchy to the target Configuration Manager 2012 hierarchy.

Software Distribution Packages

Software distribution packages are migrated as is. During the migration from Configuration Manager 2007, packages are not converted to the new application model. To be able to migrate the classic packages (which are supported in Configuration Manager 2012) to the new application model, you need to use Application Conversion Manager once the package has been migrated to the target Configuration Manager 2012 hierarchy. This tool will help you to migrate the classic packages to the new application model. Application Conversion Manager is discussed further in this chapter.

The central administration site or primary site in a stand-alone scenario always needs access to the Configuration Manager UNC package source path to be able to distribute and deploy the package. For this reason you will need to replace all the local package source paths in Configuration Manager 2007 with UNC paths.

Applications

Applications created in Configuration Manager 2012 are migrated with their deployment types, requirement rules, detection methods, deployments, dependencies, and all other configured settings. Like all objects with content, the source path needs to be a UNC path.

Virtual Application Packages

Virtual application packages are converted to the new application model. After the migration of the packages you will need to create a deployment. In Chapter 8, "Application Deployment," you'll learn how to create deployments for your virtual applications.

To be able to use virtual applications in Configuration Manager 2012, you need to upgrade the App-V client to at least version 4.6 SP1 with the hotfix that is described in Knowledge Base article 2645225. The App-V client 4.6 SP2 is supported as well; however, App-V 5 and App-V 5.0 SP1 are supported only in Configuration Manager 2012 SP1 and R2.

When Distribution Point Sharing is enabled, the streaming of App-V packages is not supported.

App-V Virtual Environments

App-V 5 has been supported since Configuration Manager 2012 SP1. A feature that comes with this support is the ability to create an App-V virtual environment, which creates a connection between two separate App-V applications. You can migrate those virtual environments to another R2 hierarchy.

Software Updates

Software updates can be migrated with the three different migration jobs in Configuration Manager 2012. You must be sure that all the updates that are available within the source Configuration Manager site are also available in Configuration Manager 2012 and ensure that the software update point is configured. Making the same software updates available in Configuration Manager 2012 can be done as follows:

Use Export and Import of Software Updates Use the tool `wsusutil.exe` to export the software updates from a source Configuration Manager site server and to import the software updates in Configuration Manager 2012. This option is the most common option to use when migrating the software update source to Configuration Manager 2012.
To export and import software updates using `wsusutil.exe`, perform the following steps:

1. Start the command line at the Configuration Manager 2007 Software Update site server, and go to

   ```
   C:\Program Files\Update Services\Tools
   ```

2. Start the `wsusutil.exe` export:

   ```
   WSUSUTIL.exe export .\cm2k7updates.cab .\import.log
   ```

3. Check the log file, and copy the exported CAB file to the Configuration Manager 2012 Software Update site server.

4. Start the command line at the Configuration Manager 2012 Software Update site server, and enter

   ```
   C:\Program Files\Update Services\Tools
   ```

5. Start the `wsusutil.exe` import:

   ```
   WSUSUTIL.exe import .\cm2k7updates.cab .\import.log
   ```

After the source is migrated, you may migrate the Configuration Manager 2007 objects to Configuration Manager 2012. For the conversion of the Software Update objects, the following rules apply:

- Update lists are converted to update groups.
- Software update deployments are migrated to deployments and update groups.
- While migrating from Configuration Manager 2012, software update groups can also be migrated.
- Automatic deployment rules can be migrated from a Configuration Manager 2012 site.

Operating System Deployment

The following operating system deployment–related objects in Configuration Manager are suitable to be migrated to Configuration Manager 2012:

- Boot images
- Driver packages

- Drivers
- Images
- OS installers
- Task sequences

Not all operating system deployment–related objects are supported for migration to Configuration Manager 2012:

- Migration of Microsoft Deployment Toolkit task sequences is not supported.
- The default Configuration Manager 2007 boot images are not migrated because the new Windows Assessment and Deployment Kit (ADK) that is supported in Configuration Manager 2012 supplies the version-matched boot images.

Customized Boot Images

Boot images that have been customized cannot be migrated. The migration process will replace the customizations made in the boot image with the default settings from Configuration Manager 2012 boot images. A new boot image ID is assigned to each boot image. The newly created boot image can be accessed only from Configuration Manager 2012 distribution points.

When migrating a boot image that has drivers embedded, be sure that the drivers remain available from the Configuration Manager 2007 source location. Configuration Manager 2012 must also be able to access the drivers from its specified source location.

Configuration Manager 2012 removes all the references to operating system client packages from the migrated task sequences. After the migration of the task sequence is finished, you can edit them in the Configuration Manager 2012 console to restore references to the local client installation packages in the target Configuration Manager 2012 hierarchy.

When migrating the operating system deployment functionality, you need to be sure that the dependent Configuration Manager 2012 site roles are installed and configured. The state migration point needs to be configured, and the distribution points must support PXE. You can read more about configuring operating system deployment in Chapter 10, "Operating System Deployment."

Settings Management

Configuration baselines and configuration items created by you as an administrator or created by an independent software vendor are supported for migration by the migration feature of Configuration Manager 2012.

When you need to re-migrate configuration items or baselines, any changes to the objects will be added as revisions of the objects.

Existing 2007 or 2012 configuration packs can also be added to 2012 through the import feature. The Configuration Manager 2012 import feature will automatically convert the 2007

schema to the 2012 schema. Keep in mind the following migration rules when migrating configuration baselines and configuration items:

- When migrating a configuration baseline, its assignment will not be migrated at the same time. You must migrate the configuration baseline assignment separately by using the collection migration job type.
- Configuration items in Configuration Manager 2007 might have rules that are not supported by Configuration Manager 2012. When you migrate configuration items that have unsupported rule operators, Configuration Manager 2012 will convert them to equivalent values.
- If the objects and settings of an imported configuration item are not visible in the Configuration Manager 2007 console, also known as incomplete or uninterpreted configuration items, they are not supported by Configuration Manager 2012. For this reason you are not able to migrate these configuration items.

Asset Intelligence Customizations

You can migrate asset intelligence customizations made for classifications, labels, families, and hardware requirements to Configuration Manager 2012. This is done by using the Object Migration option in the migration feature.

When migrating Asset Intelligence customizations, always assign the Configuration Manager 2012 site that is the closest to the Configuration Manager 2007 site that owns the Asset Intelligence content because of WAN traffic that can occur during the migration. Gathered Asset Intelligence data is not migrated to Configuration Manager 2012.

Software Metering Rules

Software metering rules can be migrated with the Object Migration option in the migration feature. All rules that are available in the source Configuration Manager hierarchy can be migrated.

After the migration all software metering rules are disabled by default.

Saved Searches

In the Configuration Manager 2012 administrative console saved searches can be migrated.

Search and Administrative Folders

Administrator-created folders for administrative duties are migrated if chosen while migrating collections or objects. Be sure to enable the Transfer The Organizational Folder Structure For Objects From The Source Hierarchy To The Destination Hierarchy option when migrating objects from Configuration Manager 2007 to Configuration Manager 2012. You can set this option in the process of creating a migration job and scheduling when the migration job is to run.

Reports

When you want to migrate reports, the only way to do so is to use SQL Reporting Services in Configuration Manager 2007 instead of the default web reporting of Configuration Manager 2007. With SQL Reporting Services you can export your custom reports (RDL files) from

the old SQL Reporting Services and then import them into your new SQL environment in Configuration Manager 2012. Migrating reports in this manner is outside the scope of the built-in Configuration Manager migration tasks.

Objects Not Supported for Migration

Not all objects can be migrated by the migration feature from a source Configuration Manager hierarchy to Configuration Manager 2012. You can create workarounds for some objects, but for others you cannot. Table 3.1 shows whether workarounds are available for non-migratable objects.

Table 3.1: Workarounds for non-migratable objects

Object	Workaround
Queries	Export the queries in Configuration Manager 2007 to a MOF file and import the MOF file into Configuration Manager 2012.
Security rights for the site and objects	No workaround available.
Configuration Manager 2007 reports from SQL Server Reporting Services	Export your reports from SQL Server Reporting Services and import them into the new SQL Server Reporting Services servicing the Configuration Manager 2012.
Configuration Manager 2007 web reports	No workaround available.
Client inventory and history data	No workaround available.
AMT client provisioning information	No workaround available.
Files in the client cache	No workaround available.

Preserving Your Custom SMS_DEF.MOF Investments

The migration of hardware inventory is not supported, but you can import your custom `SMS_DEF.MOF` files into the new Configuration Manager 2012 infrastructure. Analyze and test the custom MOF edits before importing them into the production environment of Configuration Manager 2012, and ensure that there are no conflicting data types in Configuration Manager 2012. You will need to carefully select only those classes that you want to migrate, because many of the objects from the source hierarchy might already be defined at the target Configuration Manager hierarchy.

Distribution Point Sharing

In the process of migrating your Configuration Manager objects and clients in your source hierarchy to Configuration Manager 2012, you can use distribution point sharing. This feature allows Configuration Manager clients to retrieve content for migrated packages that are hosted on the Configuration Manager distribution points in your source hierarchy.

To do this, you will need to configure distribution point sharing on a site-by-site basis. This can be done while configuring the source hierarchy by enabling the Enable Distribution-Point Sharing For This Source Site option or by configuring the source hierarchy later by enabling the Configure option in the ribbon for the source hierarchy object.

After the data-gathering process is finished, you'll see all the distribution points, including branch distribution points and distribution point shares. Boot images and App-V applications are not supported on shared distribution points. You will need to migrate those objects in the standard manner and make them available on a Configuration Manager 2012 distribution point. As mentioned earlier, associated boundaries are migrated when you enable distribution point sharing.

A shared distribution point can be reassigned to another site without the need to reinstall the distribution point and redistribute the content.

Interoperability with Configuration Manager 2007

The migration feature in Configuration Manager 2012 gives you a level of interoperability while migrating your Configuration Manager 2007 infrastructure. Since you have two Configuration Manager hierarchies to maintain, it's a good idea to look at some interoperability possibilities and scenarios.

Once you specify a source hierarchy for the new Configuration Manager 2012 hierarchy, by default every four hours a data-gathering process will run to collect all the information about the source hierarchy. During the migration period the source hierarchy is configured in Configuration Manager 2012, and your two Configuration Manager environments are connected to each other, providing a sort of interoperability. You can change the data-gathering frequency later if you want.

Re-migrate Updated Objects The migration process doesn't move objects to the Configuration Manager 2012 environment but instead copies and, if necessary, converts the objects to Configuration Manager 2012 standards. The original objects remain in Configuration Manager 2007 and can still be used and changed. If a change is made to an original object, the data-gathering process will detect the change, and you can re-migrate the updated object.

Distribution Point Sharing Enabling distribution point sharing allows you to share a distribution point that's available in a Configuration Manager 2007 site with Configuration Manager 2012. The migrated or new Configuration Manager 2012 clients are able to retrieve content from a shared distribution point.

Content As mentioned earlier, the file content storage location is not moved during the migration process. The source content also stays at the same location if this is a Configuration Manager 2007 site server. Be aware that you may need to migrate the source content also.

Planning a Migration

This section describes the steps required to prepare the migration from a source Configuration Manager hierarchy to Configuration Manager 2012. The newly designed Configuration Manager 2012 infrastructure must be in place. Consult Chapter 4, "Installation and Site Role Configuration,"

for information on how to install and configure the Configuration Manager 2012 environment that you designed in Chapter 2, "Planning a Configuration Manager Infrastructure."

As you define your project phases and the steps you need to take to migrate your Configuration Manager infrastructure to the new Configuration Manager 2012 infrastructure, you need to plan your migration.

Preparing Your Migration

Regardless of when you want to migrate to Configuration Manager 2012, you should prepare your source Configuration Manager infrastructure in advance to allow a smooth migration, as follows:

- Be sure that your new Configuration Manager 2012 infrastructure is in place.
- If a Configuration Manager 2007 infrastructure is in place, be sure it is at least using Service Pack 2.
- If a Configuration Manager 2012 infrastructure is in place, be sure it is at least using R2.
- Use UNC paths for the package source path. Avoid using local paths; always use UNC paths to a file share. A distributed file share can be very helpful while migrating objects from one site to another site.
- Avoid mixing users and devices in collection definitions; mixing users and devices is no longer supported.
- Avoid using collections with multiple query rules that limit different collections.
- Use different site codes in Configuration Manager 2012 than in the source Configuration Manager infrastructure; they must be unique.

Planning Your Migration Strategy

When you want to migrate a Configuration Manager infrastructure to a new Configuration Manager 2012 infrastructure, you will need to walk through a migration process that can take a long time depending on your source Configuration Manager infrastructure.

As we said in the introduction of this chapter, Configuration Manager 2012 supports side-by-side migration. This means that you need to build a new Configuration Manager 2012 infrastructure next to your current production Configuration Manager infrastructure. The best way is to define a project for your migration to the new infrastructure.

As noted in Chapter 1, "Overview of Service Management," any well-planned migration leverages a well-thought-out project plan. This should be based on a solid foundation or methodology such as the Microsoft Operations Framework (MOF).

The initial steps in any project are a typical gap analysis. They fall into three basic categories; you must ask yourself the following:

- Where are we?
- Where do we want to be?
- How do we get there?

A thorough project plan should include some or all of the following phases as well as work tasks for each phase:

Phase 1: Define and capture phase

- Create a project plan.
- Document the current environment.
- Conduct an initial risk review.
- Create business test cases.
- Finalize the business proposal.

Phase 2: Build phase

- Conduct a planning workshop.
- Install a proof-of-concept lab.
- Conduct server and workstation testing.
- Procure hardware.

Phase 3: Test phase (pilot)

- Draft a communication plan for the following groups:
  - Executive/management
  - Project team
  - Site (users)
- Build and deploy hardware and software.
- Implement change control for the pilot phase.
- Perform a pilot with the new environment.

Phase 4: Production deployment phase

- Implement change control for the production development phase.
- Deploy your new environment.

Phase 5: Review phase

- Conduct a lessons-learned workshop.
- Conduct a project-reflection session (party).

One fundamental part of a project plan that is commonly overlooked is the communication plan. This is generally used in two different ways: first, to inform users of what is changing on their desktops, but more important, as a communication vehicle to show the value that you bring to the business! Use this project to highlight the capabilities of Configuration Manager 2012 as well as the business value and insights of reporting, software updates, and software distribution. Don't be afraid to highlight the hard work of the migration team and the value that a project of this magnitude brings to the business.

Performing the Migration

Two main upgrade strategies are available to deploy Configuration Manager 2012 to an existing infrastructure:

Side-by-Side Migration A side-by-side migration creates a new Configuration Manager 2012 infrastructure that runs alongside the current Configuration Manager infrastructure. This migration allows clients to be managed 100 percent of the time while the migration is being conducted. The migration feature in Configuration Manager 2012 assists you with the migration of the Configuration Manager objects in your source infrastructure.

Wipe and Load The wipe-and-load approach is useful if the goal is to start over with change and configuration management. Thus, there will be zero data saved or migrated.

In this section, you'll learn about both types, as discussed previously.

Using the Side-by-Side Migration Strategy

In a side-by-side migration, an existing Configuration Manager 2007 implementation can function while client systems are moved from Configuration Manager 2007 to Configuration Manager 2012. This enables you to do the following:

- Use new hardware.
- Modify your existing hierarchy.
- Retain historical client data.
- Redesign the Configuration Manager hierarchy.
- Retain custom objects within Configuration Manager 2007.

Migrating to Configuration Manager 2012 can take a while, depending on the source and target Configuration Manager hierarchies. In this section the migration process is explained.

Understanding the Migration Process

After preparing the Configuration Manager infrastructure, as described in the "Planning a Migration" section of this chapter, you can proceed with the migration process. The migration process has several steps, depending on your source infrastructure. The following steps are part of the migration process:

Configure the Migration Feature You configure the migration feature by creating a source hierarchy in the Configuration Manager 2012 hierarchy. You need to connect the Configuration Manager 2012 infrastructure to the topmost site of the source Configuration Manager infrastructure.

You must also configure the gathering process. You need to configure the schedule and supply administrative access for the gathering process.

Once the gathering process is complete and other source sites have been discovered, you must configure credentials for each of the additional source sites.

Share Distribution Points Sharing distribution points allows you to postpone their migration. It also reduces network traffic when you enable this feature on remote locations. Shared distribution points can be reassigned to the target Configuration Manager site.

Create Migration Jobs Migration jobs are used to migrate objects from the source Configuration Manager hierarchy to Configuration Manager 2012. You can create one or more jobs, depending on your source Configuration Manager infrastructure.

When creating a migration job you can choose to exclude objects, assign content ownership, set the security scope, limit the collections, and change site codes in your query definitions.

The migration job does not migrate the content of your Configuration Manager objects. Configuration Manager 2012 will retrieve the content from the original source file location.

Migrating content can be started instantly but can also be scheduled to start later. When using a distributed file share as a content source, you do not need to migrate the content source location.

Monitor Migration Jobs In the process of migrating your source Configuration Manager objects to the Configuration Manager 2012 environment, it is a good plan to monitor the migration. When you select the migration job, you can monitor the migration by selecting objects in the job. Besides the in-console monitoring, Configuration Manager records migration actions in the `migmctrl.log` file located in the `Logs` (`%SMS_LOG_PATH%`) folder in the Configuration Manager 2012 installation path.

If a migration job fails and other jobs are still running, you should review the details in the `migmctrl.log` file as soon as possible. Migration actions are continually added to the file and overwrite the old details.

In the Configuration Manager console, you are able to monitor the migration by looking at the Migration dashboard, shown in Figure 3.5.

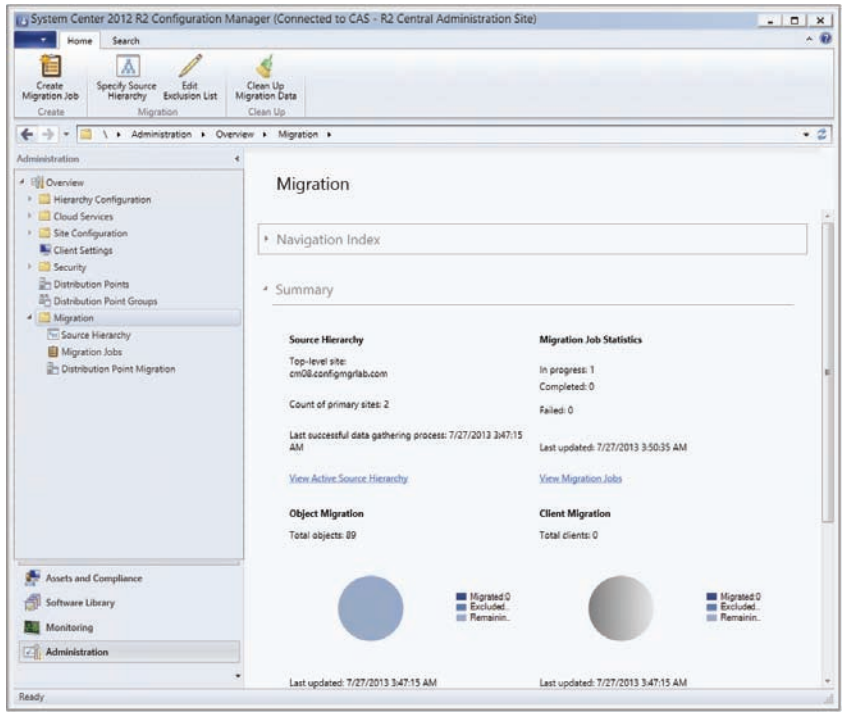


FIGURE 3.5
The Migration dashboard

Report Migration Results With the reporting feature within Configuration Manager 2012 you can report information about the migration of the Configuration Manager 2007 objects to Configuration Manager 2012. The following reports are available in the Migration category:

- Clients in Exclusion List
- Dependency on a Configuration Manager Collection
- Migration Job Properties
- Migration Jobs
- Objects That Failed to Migrate

You will find more information about reporting in Chapter 13, "Reporting."

Reassign Distribution Points When upgrading or reassigning distribution points you want to avoid having a large amount of data flowing through the WAN. For this reason, you can migrate distribution points in two ways: automatic and manual. Configuration Manager 2012 supports upgrading or reassigning the following distribution points:

- Branch distribution point
- Server share distribution point
- Standard distribution point

When you choose automatic migration, you need to enable distribution point sharing and reassign the distribution point from the Configuration Manager 2012 console. During the migration process, the distribution point is removed from the source Configuration Manager database, and the new Configuration Manager 2012 distribution point is installed on the server. If you're migrating from Configuration Manager 2007, the content of the distribution point is copied to the new content library of Configuration Manager 2012 after the installation. Be sure to have enough disk space available.

If there is a Configuration Manager 2007 secondary site available, the secondary site will automatically be uninstalled before the Configuration Manager 2012 distribution point is installed. The migration job will pause until the next data-gathering job to check if the secondary site is completely uninstalled.

One distribution point upgrade migration job is performed at a time, and other subsequent jobs are queued.

After upgrading the Configuration Manager 2007 distribution point, you need to manually delete the old content; be sure to test your deployments first.

Start Preparing Now

You can prepare for distribution point upgrades by upgrading your branch distribution points to Windows 7 in a Configuration Manager 2007 environment. Windows XP is not supported. Use the Branch Distribution Point management task to migrate it from Windows XP to Windows 7 without having to redistribute the content. To find more information about the Branch Distribution Point management task, see the online documentation of Configuration Manager 2007.

Upgrade Configuration Manager 2007 Secondary Sites Upgrading secondary sites is possible only by uninstalling the Configuration Manager 2007 secondary site and then installing the new secondary site from the Configuration Manager 2012 console.

Migrate Clients The migration of the clients is done using the same methods as for deploying a new Configuration Manager 2012 client. The first step in the migration is to uninstall the old Configuration Manager client and install the Configuration Manager 2012 client. During this process, the Configuration Manager data—for instance, advertisement history and the GUID of the client—is preserved.

Upgrade the Administrative Console The administrative console can be installed on several servers and workplaces. To be able to manage the new Configuration Manager 2012 infrastructure, you also need to upgrade the administrative console to the Configuration Manager 2012 console.

Perform Post-Migration Tasks After migrating all the old Configuration Manager 2007 content, you must perform post-migration tasks. The first task is to stop the data-gathering process, clean up the migration data, and remove the source hierarchy. Then you need to remove the old Configuration Manager 2007 infrastructure from your environment.

The step-by-step details of these procedures are provided in the following sections.

Configuring the Migration Feature

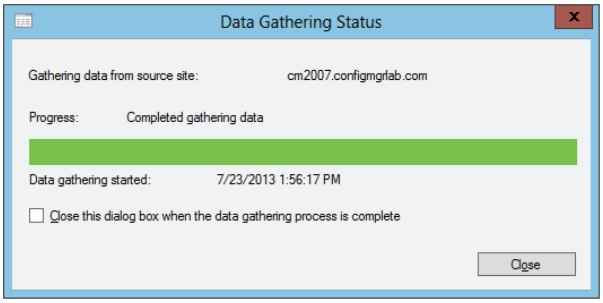
Configuring the migration feature can be done with the following steps. First, you will need to specify the source hierarchy:

1. In the Configuration Manager console choose the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Source Hierarchy.
3. Choose the Home tab of the ribbon and choose Specify Source Hierarchy.
4. In the Specify Migration Source screen, select New Source Hierarchy at the Source Hierarchy.
5. Specify the top-level Configuration Manager site server of your source Configuration Manager hierarchy by filling in the fully qualified domain name (FQDN) of the server.
6. Specify the site access account for the SMS provider of the source site server. Verify the connection of an existing or new account before submitting.

   The account needs read permissions to all source site objects.
7. Specify the site access account for the SQL server of the source site server.

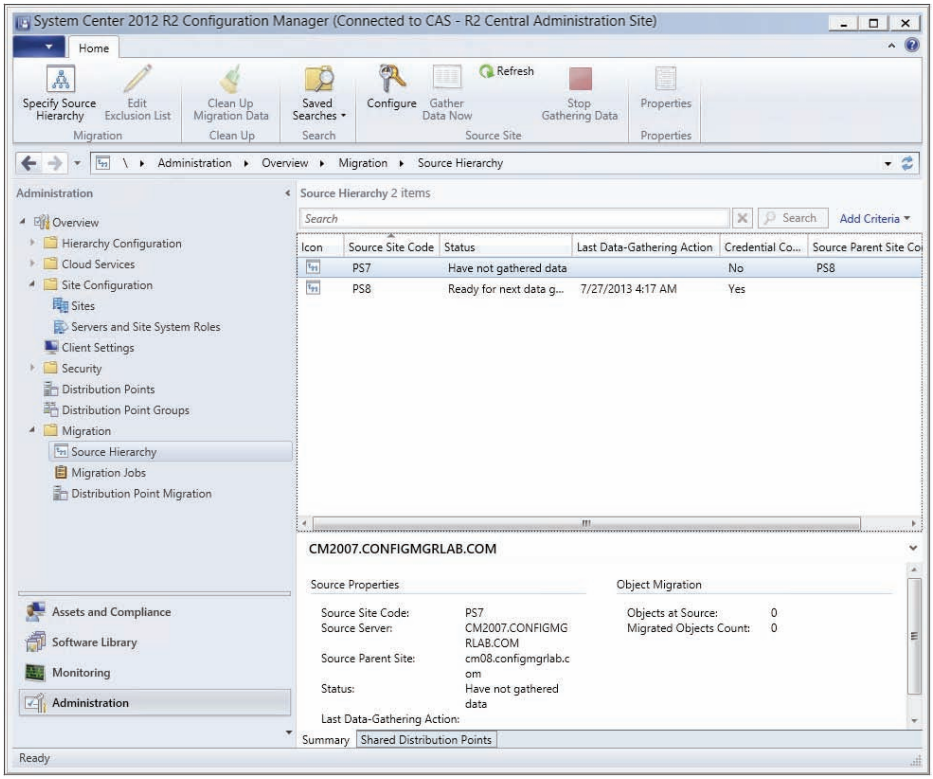
   The Windows user account needs read and execute permissions to the site database. This can be the same account that has access to the SMS provider.
8. If you want to share the distribution points in the source hierarchy, enable the option Enable Distribution Point Sharing For The Source Site Server.
9. Click OK to save the configuration and to start the data-gathering process. You'll see the Data Gathering Status dialog box, as shown in Figure 3.6.

FIGURE 3.6
The first data-gathering process is complete.



After the first data-gathering process has finished, all other primary sites in the hierarchy are discovered. In Figure 3.7 you see another primary site that has been discovered, but the data-gathering process has not run yet. The next step is to configure the credentials for the Configuration Manager 2007 source site to be able to gather the data.

FIGURE 3.7
Additional sources site discovered during the data-gathering process



1. In the Configuration Manager console choose the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Source Hierarchy.
3. Select the site with the status Have Not Gathered Data.
4. On the Home tab of the ribbon, select Configure in the Source Site section.
5. Specify the site access account for the SMS provider of the source site server.

   The account needs read permissions to all source site objects.
6. Specify the site access account for the SQL Server of the source site server.

   The Windows user account needs read and execute permissions to the site database. This can be the same account as the account that has access to the SMS provider.
7. Optionally, if you want to share the distribution points in the source hierarchy, enable the option Enable Distribution Point Sharing For The Source Site Server.
8. Click OK to save the configuration and to start the data-gathering process.

After configuring the credentials for the additional sites, the gathering process will start to gather all the objects in the Configuration Manager 2007 source site.

You can also configure the source hierarchy via native Configuration Manager 2012 PowerShell support:

1. In the Configuration Manager console, access the PowerShell console via the blue pull-down menu, and select Connect Via Windows PowerShell.
2. Type in the following PowerShell command; in this example the topmost primary site server is called cm08.configmgrlab.com and the user that is used to connect to the SQL and SMSProvider is the administrator account.

   ```
   Set-CMMigrationSource -SourceSiteServerName "cm08.configmgrlab.com"
   -SmsProviderAccount "configmgrlab\administrator" -SqlServerAccount
   "configmgrlab\administrator" -EnableDistributionPointSharing $True
   ```
3. After the command has completed, you will see that the sites have been discovered and that the first gathering process has been started.

Enabling Distribution Point Sharing

The distribution points from a selected Configuration Manager site can be shared on a per-site basis in the Configuration Manager 2012 console:

1. In the Configuration Manager console open the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and select Source Hierarchy.
3. Select the site for which you want to enable distribution point sharing.
4. Select the Home tab of the ribbon, and choose Configure.

5. In the Source Site Credentials dialog box choose the Enable Distribution-Point Sharing For This Source Site option.
6. Click OK.

After enabling distribution point sharing, the gathering process will start to gather all the objects and distribution point data in the Configuration Manager source site. Once the site servers are protected, the boundaries related to the site servers of the distribution points are migrated also.

Creating Migration Jobs

As mentioned earlier, you can create three different migration jobs. Depending on your purpose, you need to use one of the following three procedures. The three different migration jobs are designed to provide support for migrating collections with all the related objects and to provide support for migrating one or more objects or objects that are changed after being migrated.

Creating a Collection Migration Job

You can use a collection migration job to migrate the collections with objects that are associated with the specific collections. This job is available only when migrating from Configuration Manager 2007 to Configuration Manager 2012. To create a collection migration job, follow these steps:

1. In the Configuration Manager console select the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Migration Jobs.
3. Select the Home tab of the ribbon, and choose Create Migration Job.
4. Give the migration job a name and description.
5. Select Collection Migration as the job type, and click Next.
6. Select the collections that you want to migrate, as shown in Figure 3.8, and select Migrate Objects That Are Associated With The Specified Collections.

   Another option instead of "pick and choose" is to search for the collection(s) that you want to migrate. This is done by clicking the Search button and searching for the collection based on the collection name, site code, collection ID, or status. You can review the collections that cannot be migrated by clicking the View Collections That Cannot Migrate button, also shown in Figure 3.8.
7. After searching or selecting the collections, click Next.
8. Review the objects that will be migrated, make changes if necessary, and click Next.
9. Select the destination site that will be the owner of the objects, and click Next.
10. Configure the security scope, and click Next.
11. Limit the collections if needed, and click Next.

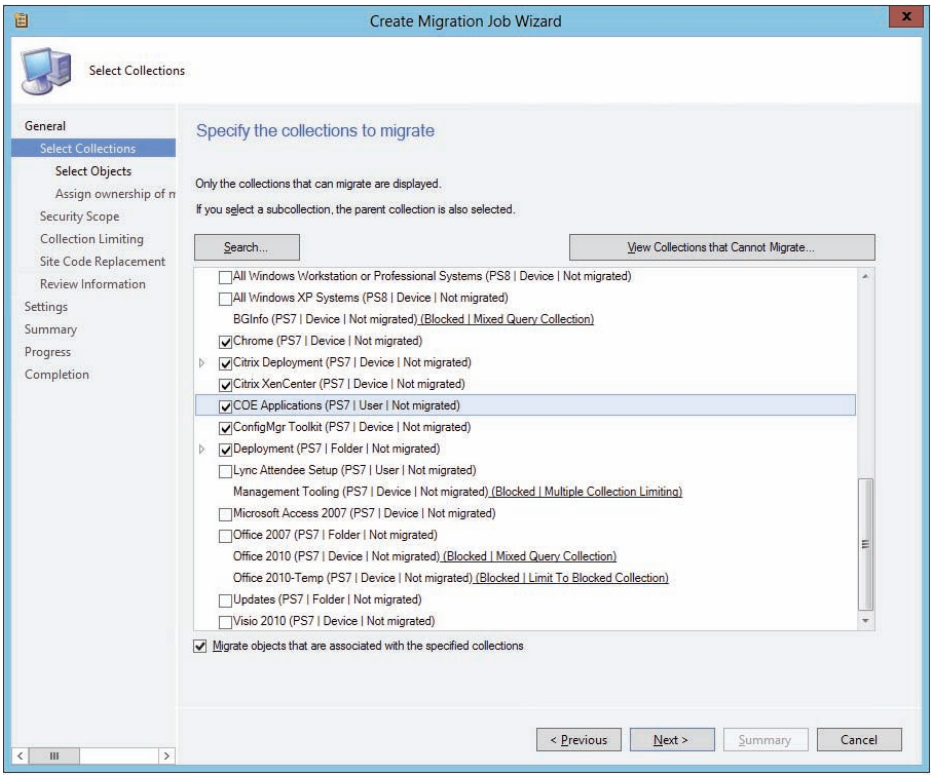


FIGURE 3.8 Selecting the collections that need to be migrated

12. Replace the site code, and click Next.
13. Review the migration job information, optionally save it to a file, and click Next.
14. Select the schedule, configure the conflict handling and additional settings for the migration job, and click Next.
15. Confirm the settings on the Summary screen, and click Next.
16. Click Close to monitor the migration of the collections and the related objects.

Creating an Object Migration Job

Object migration jobs are used for migrating one or more Configuration Manager objects to Configuration Manager 2012. This method is supported for both Configuration Manager 2007 and Configuration Manager 2012 source hierarchies. To create an object migration job, perform the following steps:

1. In the Configuration Manager console select the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Migration Jobs.

3. Select the Home tab of the ribbon, and choose Create Migration Job.
4. Give the migration job a name and description.
5. Select Object Migration as the job type, and click Next.
6. Select the objects that you want to migrate, as shown in Figure 3.9.

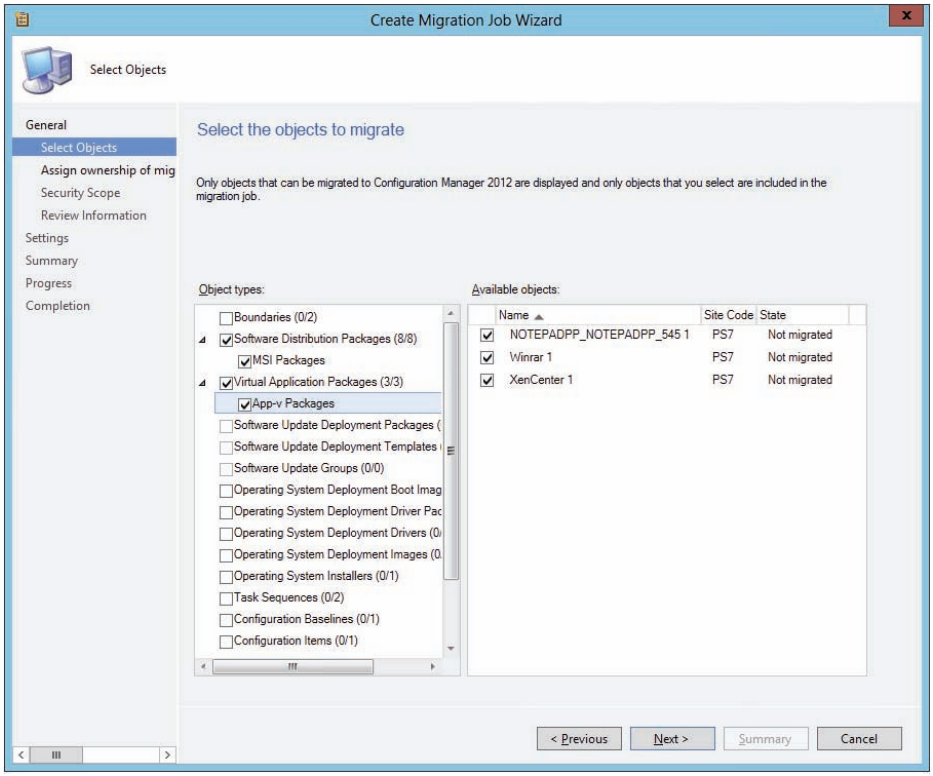


FIGURE 3.9
Select the objects that need to be migrated.

7. Click Next.
8. Select the destination site that is going to be the owner of the objects, and click Next.
9. Configure the security scope, and click Next.
10. Review the migration job information, optionally save it to a file, and click Next.
11. Select the schedule, configure the conflict handling and additional settings for the migration job, and click Next.
12. Confirm the settings on the Summary screen, and click Next.
13. Click Close to monitor the migration of the objects.

Creating an Object Modified After Migration Job

During a lengthy migration process, objects in the Configuration Manager 2007 infrastructure will change. With the objects modified after migration job, you can re-migrate the changed objects. Follow these steps to create an Object Modified After Migration job:

1. In the Configuration Manager console open the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Migration Jobs.
3. Select the Home tab of the ribbon, and choose Create Migration Job.
4. Give the migration job a name and description.
5. Select Object Modified After Migration as the job type, and click Next.
6. Select the objects that you want to re-migrate, as shown in Figure 3.10, and click Next.

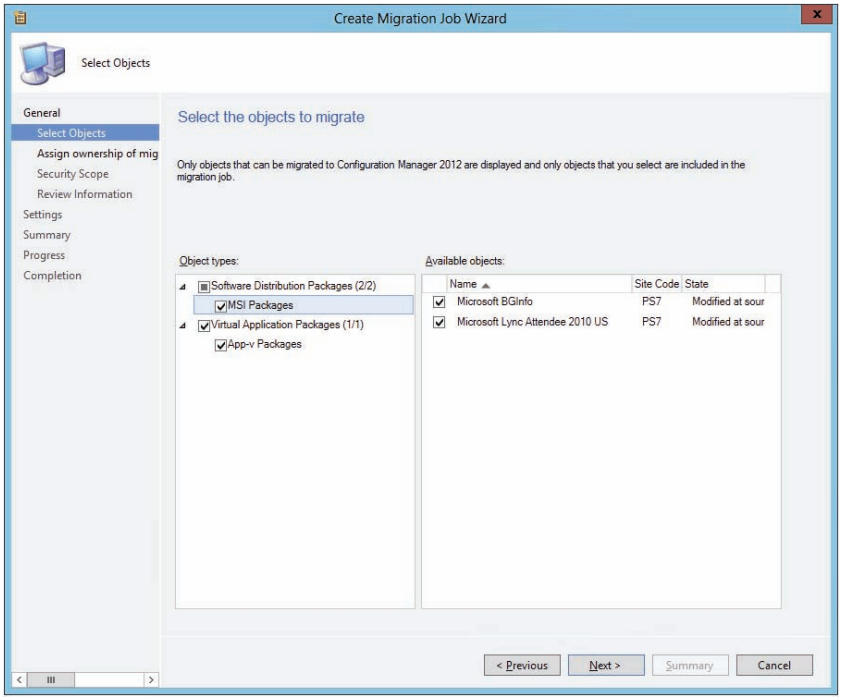


FIGURE 3.10 Select the changed objects that need to be re-migrated.

7. Select the destination site that will be the owner of the objects, and click Next.
8. Configure the security scope, and click Next.
9. Review the migration job information, optionally save it to a file, and click Next.
10. Select the schedule, and click Next.
11. Confirm the settings on the Summary screen, and click Next.
12. Click Close to monitor the migration of the changed objects.

Upgrading Distribution Points

Migrating distribution points can be done in two ways:

- Automatically
- Manually

The procedures for both options are described in the following sections.

Migrating Distribution Points Automatically

Migrating a distribution point can be done automatically by removing the distribution point from the source database and adding it to the target database. It is supported only when no site roles other than a management point of a secondary site are active. You must remove the other roles such as software update points, PXE service points, or state migration points before proceeding. To be able to migrate the distribution point, you need to enable the site for distribution point sharing.

You can upgrade the distribution point by following this procedure:

1. In the Configuration Manager console, choose the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Source Hierarchy.
3. Select the source site and choose the Shared Distribution Points tab in the information pane at the bottom of the console.
4. Select the Configuration Manager distribution point that you want to migrate or reassign to the new Configuration Manager 2012 site.
5. Select the Distribution Point tab of the ribbon, check to see if the distribution point is eligible for reassignment, and choose Reassign Distribution Point. If the distribution point is not eligible for reassignment, site roles other than those described earlier are active on the selected distribution point.
6. In the Reassign Shared Distribution Point Wizard choose the site code where the distribution point must connect after upgrading. At this point, if the distribution point must be available from the Internet, configure it by filling in the FQDN for the site system for use on the Internet. Click Next.
7. Configure the distribution point settings by choosing whether the setup must install and configure IIS, if it is required, and configure whether the distribution point can handle prestaged content. Click Next.
8. Configure the drive settings for the distribution point that will be upgraded, and click Next.
9. If you want to use the pull distribution point method to pull the content from another distribution point, you can enable this option. Otherwise, click Next.
10. Configure PXE support if needed, and click Next to configure content validation for this distribution point. Click Next to proceed.
11. Configure boundary group membership for the new Configuration Manager 2012 distribution point, and click Next.

12. Be sure you have enough free space to proceed with the upgrade. Check to see if the required space meets the available space on your configured drives, as shown in Figure 3.11. When migrating a distribution point, the content located at the distribution point is copied and converted to the new content library. Click Next if you are sure that there is enough space available.

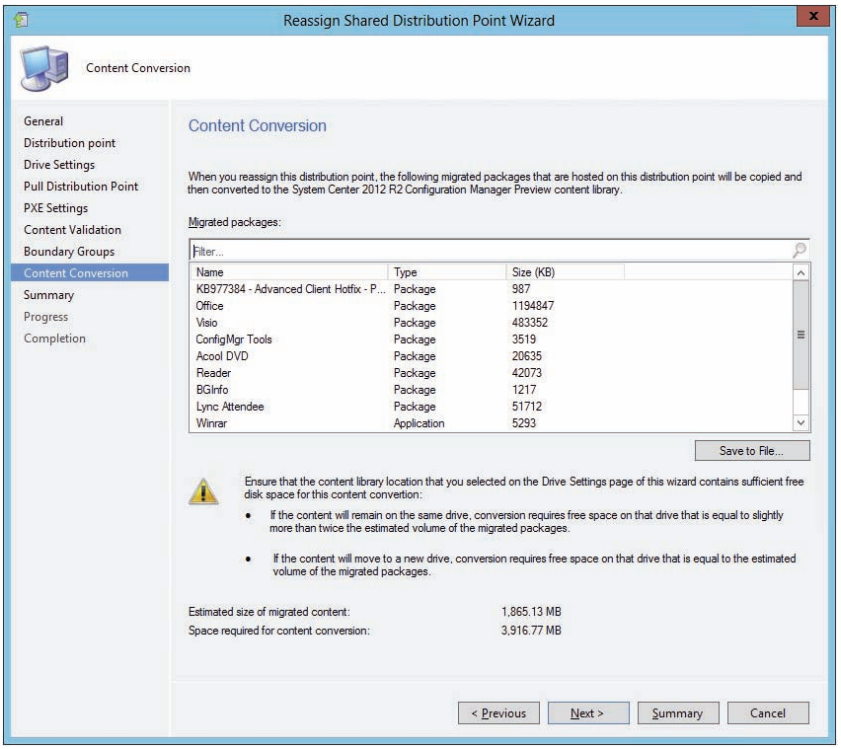


FIGURE 3.11
Be sure you have enough disk space for converting packages to the new content library.

13. Review the Summary screen, and click Next to process the upgrade.

You can monitor the migration process in the `migmctrl.log` file in the `Logs` (`%SMS_LOG_PATH%`) folder in the Configuration Manager installation folder and in the Application log in the event viewer on the target server. Also, the target server contains a folder called `..\SMS_DP$\SMS\Logs\` and a file called `SMSDPPROV.LOG` where you can find possible errors in the installation of the distribution point. You can also view the status in the Distribution Point Migration node, as shown in Figure 3.12. Refreshing the screen will update the status of the upgrade.

The content is copied and converted to the new content library with single-instance storage. Be sure to delete the old content from the old distribution point since the old content is not removed automatically.

Refer to Chapter 4 for more in-depth information about installing and configuring distribution points.

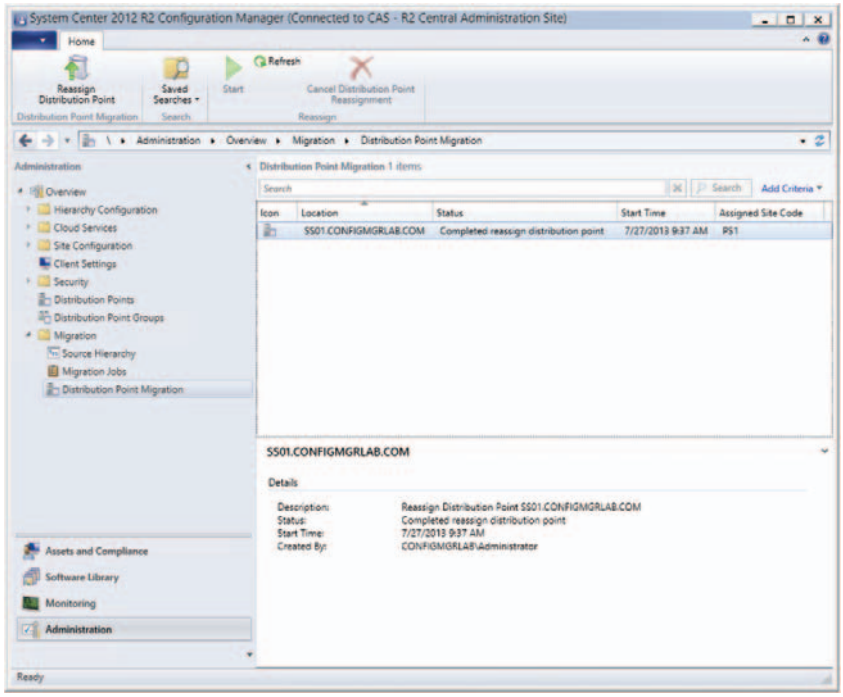


FIGURE 3.12
Monitor the upgrade status.

Migrating Distribution Points Manually

The manual migration of a Configuration Manager 2007 distribution point is done in two general steps:

1. Uninstalling the current distribution point from the Configuration Manager 2007 environment
2. Installing the distribution point with prestaged content in the new Configuration Manager 2012 environment

This scenario can be used for all distribution points, including branch distribution points, distribution point shares, and normal distribution points. For in-depth distribution point installation and configuration instructions, please consult Chapter 4.

To uninstall a distribution point from Configuration Manager 2007, follow these steps:

1. In the Configuration Manager 2007 console, open the site under Site Database\Site Management\<the site>\Site Settings, expand Site Systems, and select the site system with the distribution point.
2. Select ConfigMgr distribution point or distribution point share, and click Delete in the Actions area of the console.

To uninstall a distribution point from Configuration Manager 2012, follow these steps:

1. In the Configuration Manager console open the Administration workspace.
2. Expand Overview ➢ Site Configuration in the Administration workspace, and choose Servers and Site System Roles.
3. Select the site server with the distribution point that you want to remove, select the Distribution Point role in the Site System Roles pane, and choose Remove Role in the Site Role tab of the ribbon.
4. Click Yes to remove the distribution point.

To install a distribution point with prestaged content in Configuration Manager 2012, perform the following procedure:

1. In the Configuration Manager console open the Administration workspace.
2. Expand Overview ➢ Site Configuration in the Administration workspace, and choose Servers And Site System Roles.
3. Select the Home tab of the ribbon, and choose Create Site System Server.
4. Click Browse, and search for the server on which you want to install the distribution point.
5. Select the site code in which you want to install the site server.
6. Supply, if needed, the FQDN for use on the Internet.
7. If the server is in a different Active Directory forest, select Require The Site Server To Initiate Connections To This System.
8. Supply the site system installation account, and click Next.
9. Configure the Proxy settings, and click Next.
10. Select the Distribution Point option, and click Next.
11. Select Install And Configure IIS If Required By Configuration Manager, supply a description, and configure how the client computers are allowed to communicate with the distribution point.
12. Import, if necessary, the certificate, or choose the option Create Self-Signed Certificate.
13. Enable the option Enable This Distribution Point For Prestaged Content, and click Next.
14. Configure the Drive settings, and click Next.
15. Click Next on the Pull Distribution Point page, since you are retrieving the content from a prestaged source.
16. Configure PXE, and click Next.
17. Configure Multicast, and click Next.
18. Configure Content Validation, and click Next.
19. Configure Boundary Groups, and click Next.
20. Review the Summary screen, and click Next.
21. Click Close.

Since the distribution point is enabled for prestaged content, you can now create prestaged content packages that you need to deploy on the new distribution point. Content that can be prestaged includes the following:

- Applications
- Packages
- Software deployment packages
- Driver packages
- Operating system images
- Operating system installers
- Boot images
- Task sequence—content referenced by the task sequence

Creating prestaged content packages can be done as follows:

1. In the Configuration Manager console choose the Software Library workspace.
2. Select a content package that needs to be prestaged, and save the PKGX files to an external disk.

The next step is to extract the created PKGX files to the remote distribution point:

1. Open a command prompt in administrative mode on the server that serves as the new distribution point.
2. Switch the command prompt to the directory where you find the `ExtractContent.exe` command-line utility at `..\SMS_DP$\sms\Tools`.
3. Copy the PKGX file you just created to a folder on the new server holding the distribution point role.
4. Execute the following command, and you will receive results like those shown in Figure 3.13.

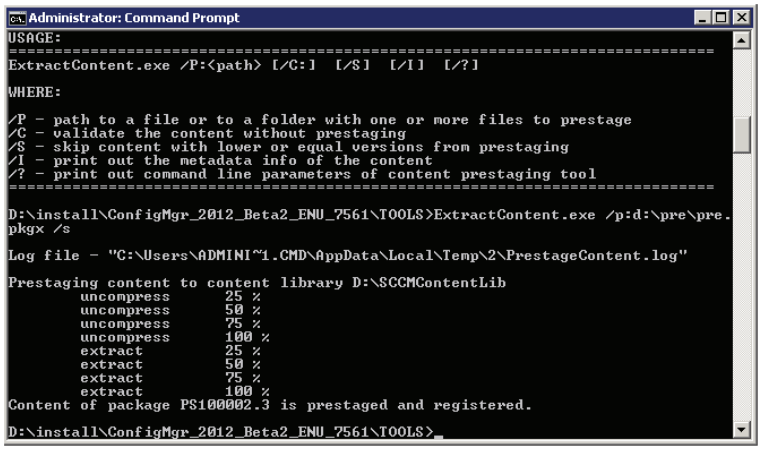


FIGURE 3.13
Extracting the prestaged package file to the new distribution point

```
ExtractContent.exe /p:<location of the prestaged
file>\<prestagedfile>.pkgx /c
```

The extraction to the distribution point will be processed in the background. For troubleshooting purposes or to follow the process, you can monitor the `PrestageContent.log` file, which you can find in the `temp` folder of your user account.

Upgrading Secondary Sites

Secondary sites need to be manually uninstalled from the Configuration Manager 2007 environment; there is no upgrade path for the scenario. While planning your Configuration Manager 2012 hierarchy, consider replacing a secondary site with just a distribution point. Chapter 2 describes when you can consider replacing a secondary site with a distribution point.

1. Right-click the secondary site and click Delete.
2. Click Next.
3. Select Deinstall The Site, and click Next.
4. Review the information about the secondary site to be deinstalled (Figure 3.14), and click Finish.

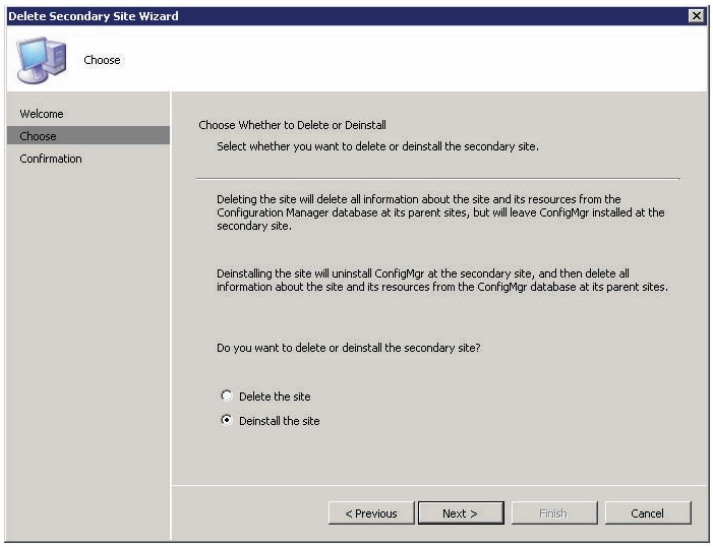


Figure 3.14 Deinstalling the secondary site from Configuration Manager 2007 SP2

After the deletion process is finished, you can install the Configuration Manager 2012 secondary site server role.

Migrating Clients

The Configuration Manager clients on the source hierarchy need to be migrated also; the process of client migration consists of uninstalling the Configuration Manager client on the devices in the source hierarchy and installing the new Configuration Manager 2012 client.

You can migrate the clients via the following methods:

- Client push installation
- Software distribution
- Group Policy
- Windows Software Update Services (WSUS)
- Manual installation
- Integration with operating system deployment

Chapter 6, "Client Installation," offers more information about client installation. The installation of the Configuration Manager 2012 client will automatically uninstall the Configuration Manager 2007 client and install the Configuration Manager 2012 client.

Remember that only the following clients are supported for Configuration Manager 2012 R2:

- Windows XP SP2 (64-bit)
- Windows XP SP3 (32-bit)
- Windows XP Tablet PC SP3 (32-bit)
- Windows Server 2003 SP2 (Standard, Enterprise, Datacenter)
- Windows Server 2003 R2 SP2 (Standard, Enterprise, Datacenter)
- Windows Storage Server 2003 R2 SP2
- Windows Server 2003 Web Edition SP2 (32-bit)
- Windows Vista SP2 (Business Enterprise, Ultimate)
- Windows 7 RTM and SP1 (Professional, Enterprise, Ultimate)
- Windows 8 (Pro, Enterprise)
- Windows 8.1 (Pro, Enterprise)
- Windows Server 2008 SP2 (Standard, Enterprise, Datacenter)
- The Server Core installation of Windows Server 2008 SP2
- Windows Storage Server 2008 R2 (Workgroup, Standard, Enterprise)
- Windows Server 2008 R2 RTM and SP1 (64-bit)
- The Server Core installation of Windows Server 2008 R2
- Windows Server 2012 (Standard, Datacenter)
- The Server Core installation of Windows Server 2012
- Windows Server 2012 R2 (Standard, Datacenter)
- The Server Core installation of Windows Server 2012 R2

A requirement of all clients is the presence of .NET Framework 4.0. You must deploy this version before migrating to the new Configuration Manager 2012 client.

Using the Wipe-and-Load Strategy

The wipe-and-load strategy is the most basic and straightforward of any of the approaches. Generally speaking, this strategy is intended for environments in which the following apply:

- You still use SMS 2003 or Configuration Manager 2007 as a single-server solution.
- None of the existing data (that is, collections, inventories, packages, and so on) needs to be retained.

Although this approach may seem like the path of least resistance, there are a few pitfalls that you need to stay aware of:

Client Manageability If you take the wipe-and-load approach, the quickest way to accomplish it is to perform a software distribution to run the `ccmclean.exe` Microsoft Resource Kit utility for SMS 2003 or Configuration Manager 2007 on all SMS 2003 or Configuration Manager 2007 clients. This poses the potential problem that the clients will remain unmanaged until the server (current or new future hardware) is rebuilt and Configuration Manager 2012 is installed and configured properly. Depending on the environment, this might be a non-issue. You would need to perform a risk assessment to see if mission-critical application updates or zero-day exploit patches need to be deployed and to assess the potential impact on your enterprise. If the risk can be minimized or negated, then a wipe-and-load operation might be possible.

Implementation Timeframe Rebuilding a server and installing or configuring all the components that are required to support a Configuration Manager 2012 installation is no small task. Not to mention that if you have a strict change-control process, this might hinder your forward momentum significantly. All these factors equate to dollars—money spent rebuilding, installing, configuring, and testing a server that was already up and running in production.

The bottom line is this: Just because the wipe-and-load option appears to be the path of least resistance, don't be tempted. Weigh your options before coming to a decision that you might regret later.

Upgrading the Configuration Manager Console

As with the Configuration Manager 2012 site server itself, you must consider the upgrade of all the Configuration Manager administrative consoles to the new Configuration Manager 2012 administrative consoles. This potentially is an area for automation or an unattended installation routine.

Any of the setup functions (primary site, secondary site, or administrative console) can be scripted with an initialization file to answer key questions of a setup routine. In this scenario, we want to automate the administrative console setup for Configuration Manager 2012.

The following steps will enable you to perform an unattended installation of the Configuration Manager 2012 administrative console:

1. Ensure that administrator workstations meet the minimum requirements for the Configuration Manager 2012 administrative console. In order to run the Installation Prerequisite Checker to verify the workstation, you can run `prereqchk.exe /ADMINUI` from the command line. You can find this file in the installation source on the DVD (`SMSSetup\Bin\x64`).
2. Advertise the setup of Configuration Manager 2012 with the following command, substituting the *<msiexec /I \SMSSETUP\BIN\i386\AdminConsole.msi /qn>* text with the name and location of the file:

   ```
   msiexec /I \SMSSETUP\BIN\i386\AdminConsole.msi /qn
   ```

The unattended installation will not remove the old Configuration Manager 2007 console. You can remove the console by uninstalling it via the Programs And Features option in Control Panel.

The following steps enable you to perform a GUI installation of the Configuration Manager 2012 administrative console:

1. Ensure that administrator workstations meet the minimum requirements for the Configuration Manager 2012 administrative console. In order to run the Installation Prerequisite Checker to verify the workstation, you can run `prereqchk.exe /ADMINUI` from the command line. You can find the file at the following folder on the System Center 2012 R2 Configuration Manager DVD: `\SMSSETUP\BIN\x64\`.
2. Insert the System Center 2012 R2 Configuration Manager DVD, browse to the `\SMSSETUP\BIN\i386\` folder, and double-click `AdminConsole.msi`.

   The Configuration Manager Console Setup Wizard appears.
3. Click Next.
4. Supply the site server name, and click Next.
5. Browse to the installation location, and click Next.
6. Choose whether you want to join the Customer Experience Improvement Program (CEIP), and click Next.
7. Click Install.
8. Review any fatal errors, other errors, or warnings that are presented (although part of your homework was to run the Installation Prerequisite Checker and address all errors), or review `ConfigMgrAdminUISetup.log` and `ConfigMgrPrereq.log` on the root of the system drive to see which errors need to be addressed.
9. Click Finish to start the newly installed Configuration Manager 2012 administrative console.

Post-Migration or Installation Considerations

Once you have performed the selected installation, it is imperative to maintain its health moving forward. The obvious choice for performance and availability monitoring is Microsoft System Center 2012 Operations Manager; for this you need to install the Configuration Manager 2012 Management Pack in Operations Manager 2012. More information about support for Operations Manager 2012 can be found in the book *Mastering System Center 2012 Operations Manager*.

1. First, review the site status from within the System Status node in the Monitoring workspace in the Configuration Manager 2012 console.
2. Review all of the site system roles to ensure that they are identified properly as well as the component status.
3. If there are any critical or red components, right-click the targeted component and select Show Messages ➢ Error.

   This produces all of the error status messages, which highlight the problems within the site.

You'll find more detailed troubleshooting coverage in Chapter 19, "Troubleshooting."

Another area of concentration should be the site settings. With the new functionality and roles within Configuration Manager, a plethora of settings need to be set up and configured. A more detailed and in-depth view of site settings is provided in Chapter 4.

After you review the new environment, you need to clean up Configuration Manager 2012 by doing the following:

- Stop the data-gathering process.
- Clean up the migration data.

Stopping the Data-Gathering Process

You stop the data-gathering process by following the next procedure. You need to first stop the data-gathering processes in all of the child sites in the source hierarchy:

1. In the Configuration Manager console open the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Source Hierarchy.
3. Select the site with data gathering enabled.
4. Select the Home tab of the ribbon, and choose Stop Gathering Data.
5. Click Yes when the Stop Gathering Data dialog box appears.
6. Repeat this for all sites in the hierarchy.

Cleaning Up Migration Data

The next step in the post-migration task is to clean up the migration data, as follows:

1. In the Configuration Manager console choose the Administration workspace.
2. Expand Overview ➢ Migration in the Administration workspace, and choose Source Hierarchy.
3. Select the topmost source hierarchy site with data gathering disabled.
4. Select the Home tab of the ribbon, and choose Clean Up Migration Data.
5. Verify that you have the right source hierarchy, and click OK when the Clean Up Migration Data dialog box appears (Figure 3.15).

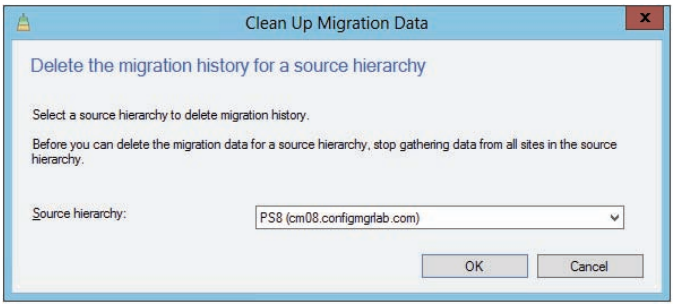


Figure 3.15 Cleaning up the migration data of the source hierarchy

Migrating Packages to the New Application Model

When you migrate your packages to Configuration Manager 2012, the classic packages are migrated as is. Configuration Manager 2012 is built around the new application model, and to get all the features of the new application model you need to convert the package to an application. You can find more information about the new application model in Chapter 8.

After migrating the packages from the Configuration Manager 2007 environment to the Configuration Manager 2012 environment, you have a couple of options for what to do with the packages:

Do Nothing You can leave the package and program as they are, since some packages are best left in the classic packages and programs format, for instance, system maintenance tools like defrag and backup. System maintenance tools are often deployed to systems instead of users. System-based classic packages cannot be converted by Package Conversion Manager since it supports only classic packages.

Convert the Packages Manually You can manually convert packages and programs to the new application model. This option is not a best practice, and it can be time consuming.

Convert the Packages with Package Conversion Manager Package Conversion Manager will lead you through the process of converting packages to the new application model. The conversion process will move the data to the application model.

The best practice is to convert the packages with System Center Configuration Manager Package Conversion Manager; this way you are able to use all features of the application model of Configuration Manager 2012.

What Is Package Conversion Manager?

Package Conversion Manager helps you analyze packages and determines the readiness for the conversion of classic packages to the new application model (see Figure 3.16). After the analysis, Package Conversion Manager will convert the package to the new application model by building applications and deployment types, and it migrates machine collection queries to the application model by building global conditions and requirement rules. The converted global conditions and requirement rules are ANDed with the program requirements. This means that the global conditions and requirement rules are merged with the classic program requirements.

While you're in the migration process, the summarization screen of Package Conversion Manager helps you identify the progress of your migration.

Package Conversion Manager is fully integrated with the Configuration Manager 2012 console, but it must be installed separately.

Not all packages are suitable for migration with Package Conversion Manager; the Manager supports the migration of packages that are *user facing,* for instance, packages that users interact with, such as these:

- MSI-based applications
- App-V-based applications
- EXE-based applications

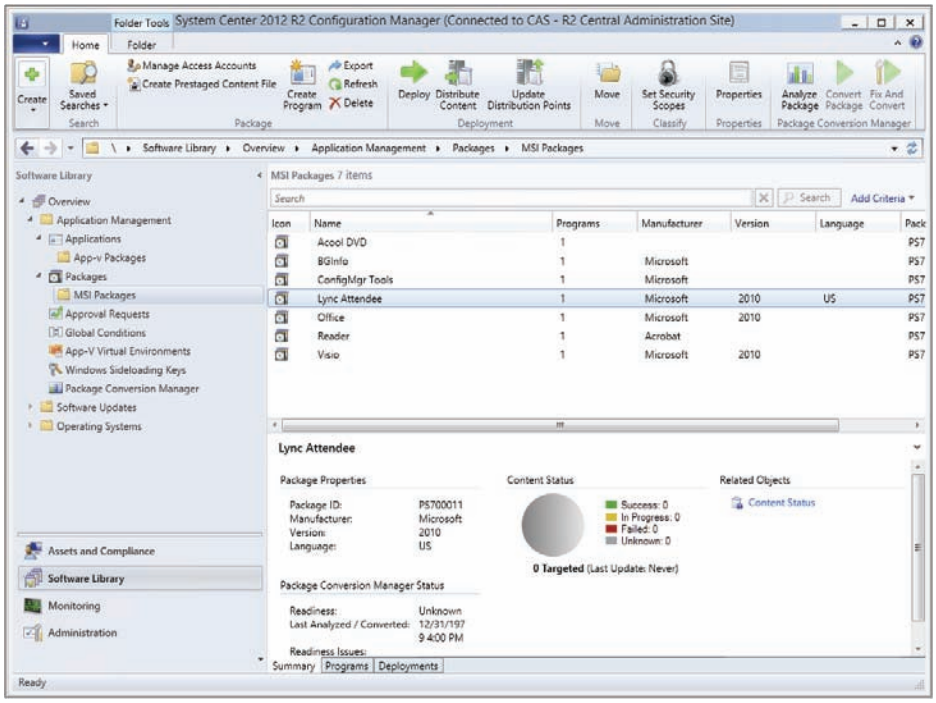


Figure 3.16 Configuration Manager console with Package Conversion Manager

Applications that are not supported or not able to be migrated include the following:

- System maintenance tools like defrag or backup
- End-of-life packages

The Conversion Process

You will need to go through the process of converting the packages and programs to the new application model. The process consists of the following phases:

- Installing Package Conversion Manager
- Analyzing the packages
- Converting the packages

Installing Package Conversion Manager

You need to install System Center 2012 Configuration Manager Package Conversion Manager 2.0 on the primary site. Package Conversion Manager is downloadable from the System Center website of Microsoft. Follow these steps to install Package Conversion Manager:

1. Close the Configuration Manager console and double-click the executable (`PCMSP1Setup-ENU.exe`) that you have downloaded from the System Center website.

2. Click Next in the Welcome screen, and accept the end-user license agreement before going further by clicking Next.
3. Click Install.
4. Click Finish after the installation is finished and restart the Configuration Manager console.

Analyzing Packages

Packages need to be analyzed before they can be converted to the new application model. Analysis of packages can done in four ways:

- You can analyze a single item.
- You can analyze in bulk by selecting additional packages.
- You can analyze during the conversion process automatically.
- You can schedule bulk analysis during nonpeak hours.

Although you can run the analysis today to see if the packages are compliant for conversion, you can migrate the packages at a later stage because while the conversion process is running, the packages will be reanalyzed.

Changing the Columns of the Packages List

If you want to view the status of the packages in the packages list, you can add the appropriate columns to the packages list. This is done by right-clicking the columns and selecting the Readiness and Last Analyzed/Converted columns.

The analysis process can result in the following readiness states of the to-be-converted packages in the Package Conversion Dashboard, as shown in Figure 3.17.

Unknown Analysis has not been run for this application.

Automatic The package can be automatically converted to the application model. This is the best state to use for bulk migrations.

Manual There is not enough data available to convert the package automatically. The administrator needs to supply input for the conversion. You may need to supply information such as detection methods and the deployment type preference order through a wizard supplied by Package Conversion Manager. A package may need to be converter manually when one of the following conditions apply:

- Package contains multiple programs.
- Package is not a Microsoft Installer package (MSI).
- Package content is not available.
- Package contains dependencies.

Not Applicable The Package Conversion Manager tool is not able to do anything with the package in this state. You may need to modify the source package in order to convert the package to the new application model.

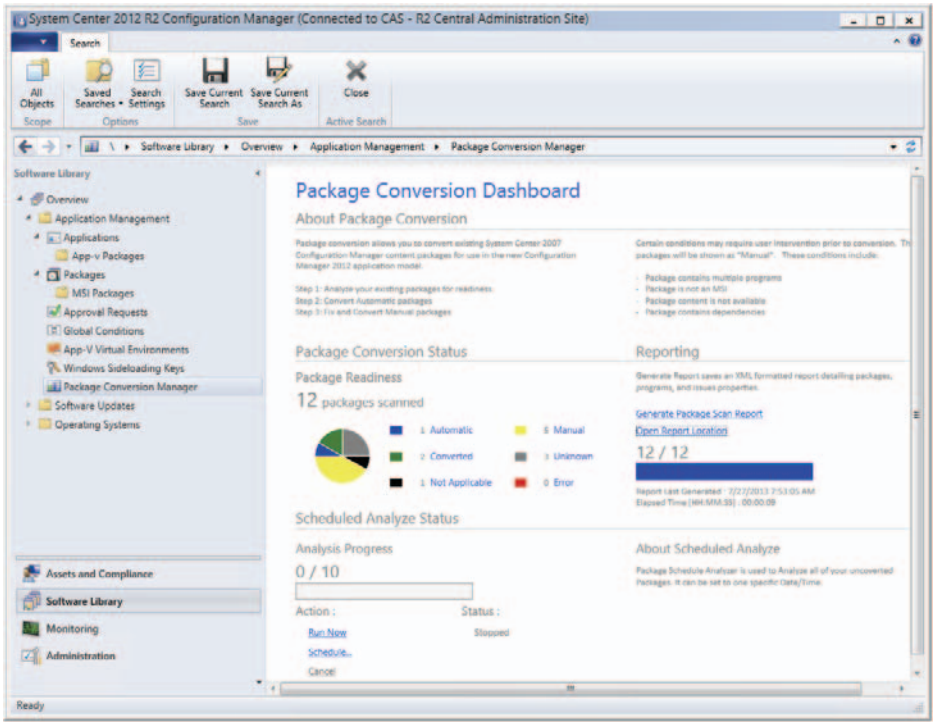


FIGURE 3.17 Package Conversion Dashboard

Converted The package has been converted to the application model. The application is manageable through the Configuration Manager 2012 console.

Error If there is an error reported, go to the package, select it, and view the summary to see the readiness issues. For instance, quote marks are not supported in the command line of the program.

If you need to convert the package, you need to be sure of the following:

- The content of the package is present.
- It is a software distribution package.
- It contains at least one program.

If one of these three must-haves is not present, then the application is not applicable. If the three are confirmed, you can migrate the application manually. You can use an automatic migration when the three must-haves are present and you have only one MSI per package available, the content is accessible, and there are no unconverted dependencies.

Automatic Conversion

Once you finish the conversion process, the application is ready for testing. The application is not fully ready for deployment yet because you still need to provide detection methods and configure the deployment type preference order.

All packages need to be analyzed before you can convert the packages and programs to the new application model. The option Convert Package is grayed out until the analyzing phase is finished.

To manually analyze packages, perform the following steps:

1. In the Configuration Manager console open the Software Library workspace.
2. Expand Overview ➢ Application Management ➢ Packages, and select one or more classic packages.
3. Select the Home tab of the ribbon, and choose Analyze Package in the Package Conversion Manager section.

If you want to schedule the analyzer to analyze the packages off peak hours, you can schedule analyzing the classic packages by following the next steps:

1. In the Configuration Manager console open the Software Library workspace.
2. Expand Overview ➢ Application Management ➢ Package Conversion Manager.
3. In the Package Conversion Dashboard click the Schedule link. Set the schedule by supplying a date and time before clicking OK.

In the notification area of the taskbar you will see an icon for the schedule; by clicking the icon you can cancel the schedule if necessary.

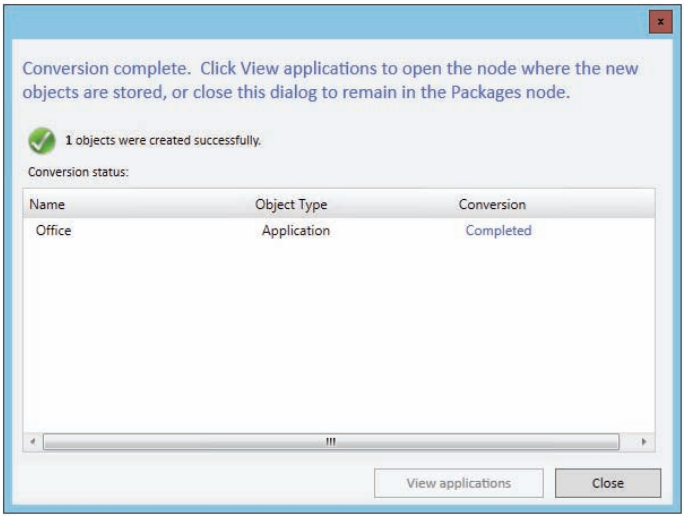
Converting the Package

When the package is analyzed and the readiness state changes from Unknown to Automatic or Manual, you can convert the packages and programs to the new application model. Packages that have an Automatic readiness state can be converted as follows:

1. In the Configuration Manager console select the Software Library workspace.
2. Expand Overview ➢ Application Management ➢ Packages, and select one or more classic packages that have an Automatic readiness state.
3. Select the Home tab of the ribbon, and choose Convert Package in the Package Conversion Manager section.
4. Review the programs and confirm the conversion of the selected packages into new application objects. Click OK.

   After the conversion progress dialog box closes, you will see a dialog box with the results of the conversion.
5. Click Close and review the converted packages in the Applications node of the Application Management workspace (Figure 3.18).

FIGURE 3.18
Conversion of the packages is complete.



During the conversion process the package is reanalyzed to be sure that the latest information about the package and program is available. The readiness state of the classic package will be changed from Automatic to Converted.

To manually convert packages and programs, follow these steps:

1. In the Configuration Manager console choose the Software Library workspace.
2. Expand Overview ➢ Application Management ➢ Packages, and select one or more classic packages that have a Manual readiness state.
3. Choose Fix And Convert in the Package Conversion Manager section of the Home tab of the ribbon.
4. Review the items to fix in the Package Selection screen of the Package Conversion Wizard, and click Next.
5. Review dependencies on unconverted packages and possible issues, and click Next.
6. Review the deployment types associated with the new application, and fix possible issues.

   In Figure 3.19, you see that there is an issue with the detection method. To fix this, select Deployment Type and then click Add to configure a detection method. In this case, an MSI product code is missing, so select Windows Installer as the Setting Type and browse to the MSI to retrieve its product. Click OK twice and check to see if the issue is fixed.
7. Click Next to review the Requirements Selection screen and check the requirements to add to the selected deployment type; then click Next.
8. Review the Summary screen and click Next. After the Package Conversion Wizard has completed successfully, click Close. You will find the converted package in the applications node where all the applications reside.

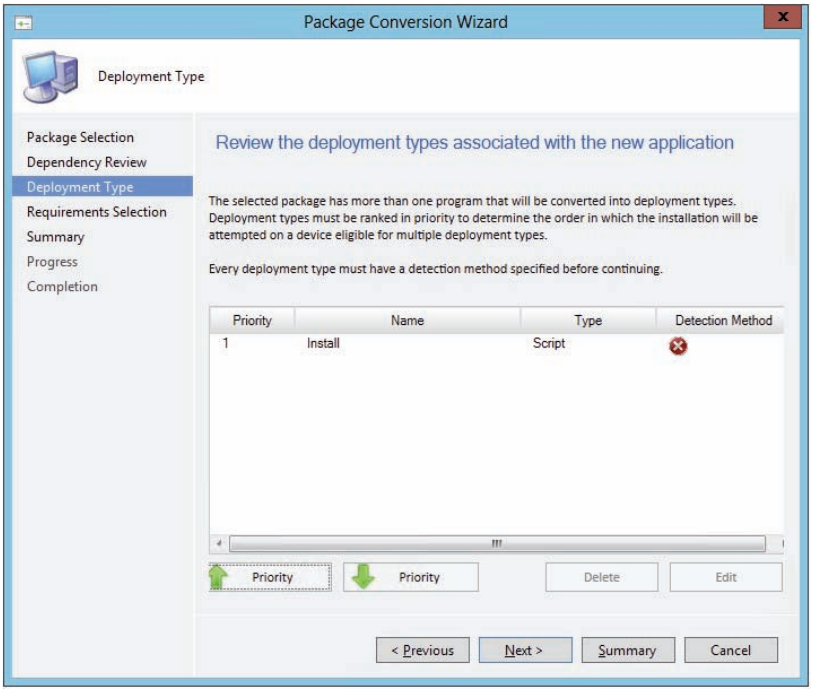


Figure 3.19 Deployment type issue

Not Applicable Classic Packages

When the readiness state of a classic package is shown as Not Applicable for a migration, you can find out why the package and programs are unable to be migrated by selecting the package and viewing the summary. As mentioned previously, there are several reasons why a package can be tagged Not Applicable.

Converting Package Dependencies

Classic packages with an unconverted dependency will have a readiness state of Manual after the first analysis. The reason is that Package Conversion Manager cannot automatically convert a package that is a dependency. You will need to first convert any package that is a dependency before converting the classic package. For instance, if you have a classic package that depends on a classic package with the .NET Framework, you need to convert the .NET Framework classic package. If you then reanalyze the classic package with the .NET Framework dependency and there are no other issues, it will be available for conversion.

The Conversion Process Steps

The conversion process does a lot of work to convert and migrate all settings to the new application model. The conversion process converts information like package properties, program properties, and MSI information. Not only such things as application name,

deployment type name, or detection method are converted, but also 28 optional properties of the packages and programs. Investments you made are preserved for the new application model.

Package Conversion Manager Best Practices

For the integration of Package Conversion Manager within Configuration Manager 2012, the following premigration and migration best practices are defined.

Premigration

You can prepare for the migration of the packages to the new application model by using the following best practices:

Utilize Platform Requirements In the package program set the platform that the program will run on. The settings are migrated as global conditions and requirements for the application.

Use the Universal Naming Convention (UNC) Path for Source Location This is required for migrating the package to an application. Otherwise, the new Configuration Manager 2012 site server cannot access the source content.

Use Only MSIs with One Unique Product Identification (PID) The MSIs need to have one unique PID. When creating your own MSI, include only one PID. Otherwise, the detection methods for installation of the applications won't work correctly.

Conversion Process

For the conversion process the following best practices are defined:

Convert Any Depended Classic Packages First Always convert the dependent classic packages first before converting the classic packages that are dependent on them. Depended classic packages that have a readiness state of Automatic will optionally be converted automatically.

Concentrate on Your User-Centric Applications Since Configuration Manager 2012 is user centric, be sure to concentrate on your user-centric applications. Configuration Manager 2007 was designed for system targeting, so try to find the classic packages that can interact with the user and that can be converted with Package Conversion Manager.

Keep Track of Your Efforts Use the summarization to plan the conversion of the classic packages and to keep track of your conversion process. For instance, you can check to see what percentage has converted.

Once Converted, Check Requirements Once a package is converted, check the requirements of the application to make sure that they are sufficient for the new application model.

Monitoring Conversion

Besides the Package Conversion Dashboard, shown previously in Figure 3.17, you can monitor the conversion of your packages via other ways, as shown in Table 3.2.

TABLE 3.2: Package conversion monitoring features

MONITORING FEATURE	DESCRIPTION
Package Conversion Dashboard	The dashboard shows the overall readiness/conversion state of all of your packages. This is the best way to monitor your package conversion process.
`PCMTrace.log`	This log file can be found in the temporary directory of the user. This log file consists of all information about the package conversions.
Packages node	Add the Readiness and the Last Analyzed/Converted columns to packages node view.
Packages properties	You can view the Package Conversion Manager status per package. Possible readiness issues are reported here.
Package Scan Report	From the Package Conversion Dashboard you can generate a report. This report is saved in the user's temp folder (`%TEMP%`) and is called `PackageScanReport.XML`, shown in Figure 3.20.

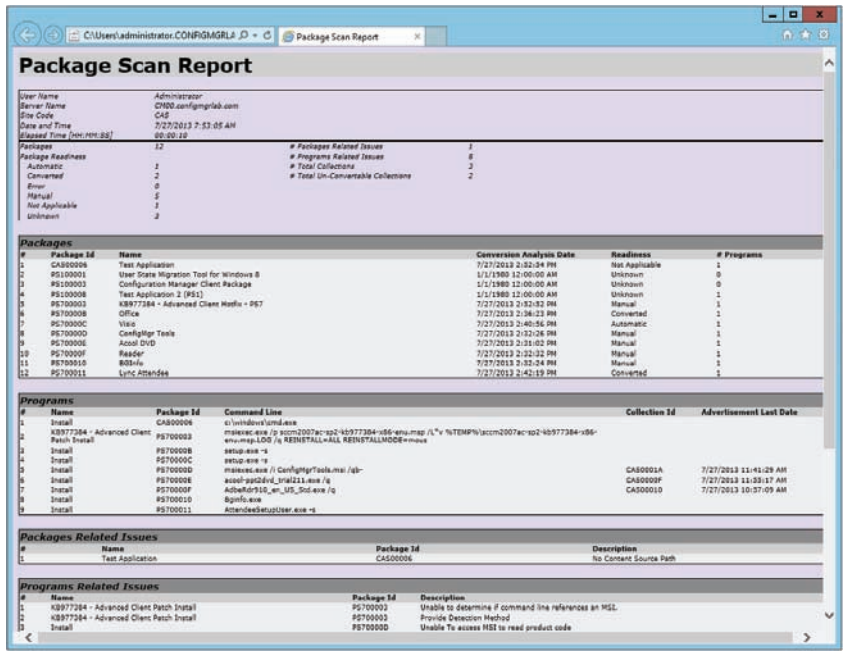


FIGURE 3.20 Package Scan Report

Migrating Branch Offices with the Physical-to-Virtual Migration Toolkit

To achieve the Configuration Manager 2012 migration goals set in the beginning of this chapter, you will need the physical-to-virtual (P2V) Migration Toolkit to maximize the reusability of x64-bit hardware. This P2V Migration Toolkit can be used when you have a branch office with limited hardware availability to perform a side-by-side upgrade.

The P2V Migration Toolkit eliminates the need for a side-by-side migration of physical servers. It enables you to host the Configuration Manager 2007 site server and the Configuration Manager 2012 site server on the same machine using virtualization with Hyper-V. The P2V Migration Toolkit uses Configuration Manager operating system deployment to create a virtual instance of the Configuration Manager 2007 site server. It uses a virtualization task sequence so that the creation of the P2V virtual machine is simplified and automated.

Requirements

The P2V Migration Toolkit requires Hyper-V to be available on the Windows Server 2008 R2 server. For virtualization with Hyper-V the following are required:

- The server must have an x64 processor.
- The BIOS must support hardware-assisted virtualization and hardware data execution prevention. Virtual machines will not start unless these features are enabled.

The P2V Migration Toolkit requires that the Configuration Manager 2007 SP2 console be installed on the workstation or server where you want to start it from. Further requirements are as follows:

- Windows 7 or Windows Server 2008 R2
- Microsoft .NET Framework 4.0 or Microsoft .NET Framework 4.0 client profile
- Windows Automated Installation Kit for Windows 7
- Desktop Experience feature in Windows Server 2008 R2

The source server that needs to be virtualized has the operating system requirements shown in Table 3.3.

TABLE 3.3: Operating system requirements for P2V conversions

OPERATING SYSTEM	EDITION	ARCHITECTURE
Windows Server 2003 SP2 or greater	Standard, Enterprise, and Datacenter	X86, x64
Windows Server 2003 R2 SP2 or greater	Standard, Enterprise, and Datacenter	X86, x64
Windows Server 2008	Standard, Enterprise, and Datacenter	X86, x64
Windows Server 2008 R2	Standard, Enterprise, and Datacenter	x64

P2V Migration Scenario

The physical-to-virtual migration is primarily used for two types of scenarios:

- It can be used for branch offices that are part of your Configuration Manager 2007 hierarchy and where you have only one piece of hardware that can be reused for Configuration Manager 2012 and that can support Hyper-V.
- It can be used for a branch office with very slow WAN links that doesn't allow an over-the-wire migration because of costs; the global SQL replication over the WAN is too expensive.

After a P2V migration of an old server is finished, you can migrate Configuration Manager 2007 and Configuration Manager 2012 side by side.

The Task Sequence

The task sequence that is used for the P2V migration scenario consists of the following tasks, resulting in a virtual machine on a new Windows Server 2008 R2 operating system. (You'll learn more about task sequences and operating system deployment in Chapter 10.)

The task sequence tasks are as follows:

1. Capture the selected physical disk partitions into virtual hard disks.
2. Install Windows Server 2008 R2.
3. Enable the Hyper-V role on the new Windows Server 2008 R2 server.
4. Set up and configure the Windows Server operating system by doing the following:
   a. Install the Configuration Manager 2007 client to be able to connect the Configuration Manager 2007 site server.
   b. Join the domain.
   c. Add predefined local administrators.
5. Prepare and compact virtual hard disks.
6. Create the virtual machine, configure the network, and attach the virtual hard disks.

Steps for Using the Configuration Manager 2012 P2V Migration Toolkit

The P2V Migration Toolkit can be used in two different ways:

- Create a task sequence with stand-alone media.
- Create non-task-sequence bootable media.

This provides flexibility in the P2V migration approach.

Creating a Task Sequence with Stand-alone Media

Use this option when you want to automate the entire end-to-end process from operating system rebuild to virtual machine creation. To create the task sequence with stand-alone media, the following four broad steps are required:

1. Create the task sequence.
2. Create stand-alone media.
3. Boot off the stand-alone media.
4. Run the task sequence.

The first step is to create the task sequence itself:

1. Start the P2V Migration Toolkit, and you will see the screen shown in Figure 3.21.
2. Click Create A Task Sequence.

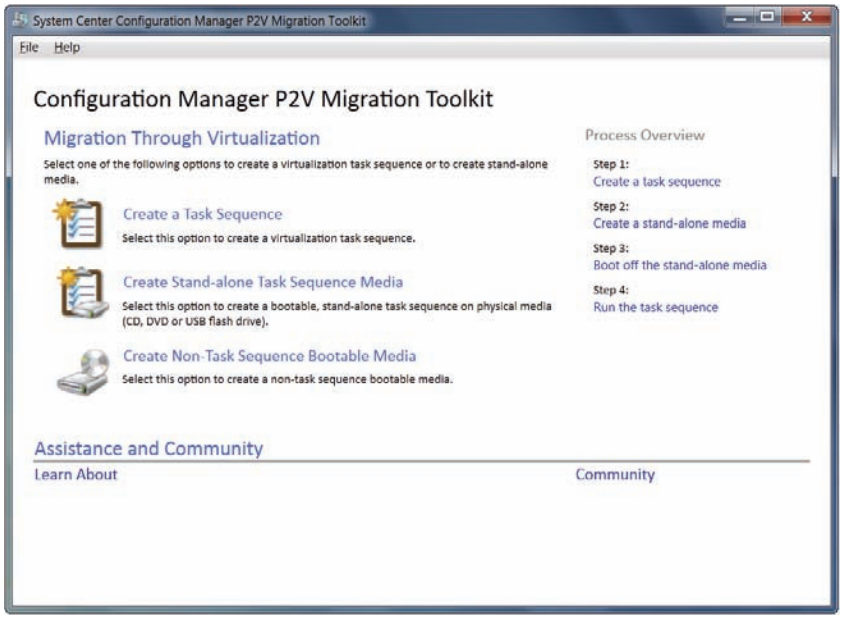


FIGURE 3.21 The P2V Migration Toolkit

3. Supply the site server name and site code, and click OK.
4. When the Task Sequence Designer launches, supply the name for the task sequence in the Task Sequence Name field.
5. Click Browse, select an existing 32-bit boot image, and click OK.
6. Click Next.
7. Click Browse, and select the Windows Server 2008 R2 image package, as shown in Figure 3.22.
8. Provide the product key and license information, and click Next.
9. Click Browse, and select Client Installation Package. Click Next.
10. Select Create New Virtualization Tools Package, or select Use An Existing Virtualization Tools Package and click Browse to select the package. Click Next.
11. If you need to create a new virtualization tools package, supply the package name, specify the deployment share, and select the distribution points where the package needs to be placed. Click Next.
12. Select Software Packages That Need To Be Installed During The P2V Installation Process, and click Next.
13. Review the Summary screen, and click Create.
14. Click Close.

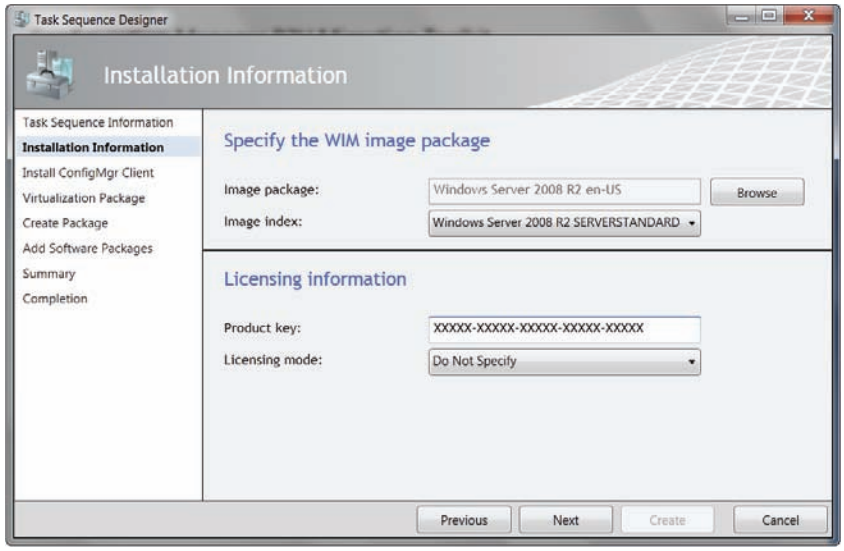


FIGURE 3.22
Specify the operating system WIM image.

The next step in the process of virtualizing the Configuration Manager 2007 site server is to create stand-alone media. The stand-alone media can consist of a USB drive or a CD/DVD set.

To create a stand-alone USB flash drive, follow this procedure:

1. Start the P2V Migration Toolkit.
2. Select Create Stand-Alone Media.
3. Supply the site server name and site code, and click OK.
4. Select USB Flash Drive.
5. Click Yes if you want to format the USB flash drive.
6. Supply a password (optional), and click Next.
7. Click Browse to select the task sequence you created earlier, and click Next.
8. Select the distribution point(s), and click Next.
9. Review the Summary screen, and click Create.
10. If the wizard has completed successfully, click Close.

To create a stand-alone CD/DVD set, perform the following steps:

1. Start the P2V Migration Toolkit.
2. Select Create Stand-Alone Task Sequence Media.
3. Supply the site server name and site code, and click OK.
4. Select CD or DVD.
5. Select the media size (650 MB, 4.7 GB, or 8.5 GB).

6. Click Browse to browse to the file location, and supply a name for the ISO file.
7. Supply a password (optional), and click Next.
8. Click Browse to select the task sequence you created earlier, and click Next.
9. Select the distribution point(s), as shown in Figure 3.23, and click Next.

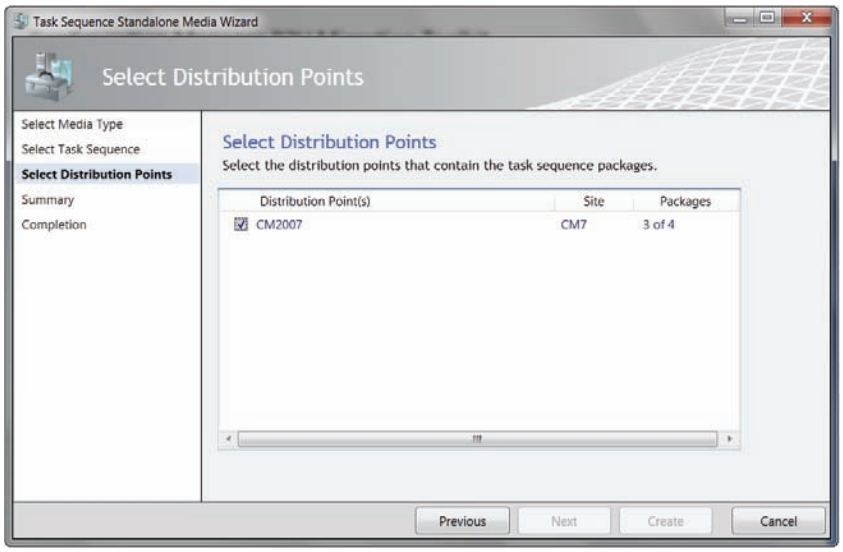


FIGURE 3.23
Be sure to place all the content on the distribution points.

10. Review the Summary screen, and click Create.
11. When the wizard has completed successfully, click Close.

The final phase of the process is to run the task sequence. Do the following:

1. Boot the branch office site server from either USB or CD/DVD.
2. Configure IP settings and supply the password if necessary; then click Next.
3. Click Next when the conformation is displayed after booting.
4. Click Next on the Welcome page of the bootable device, as shown in Figure 3.24.
5. Your system will be validated; if the system is okay, click Next.
6. Supply the computer name, domain information, and an account that will have domain join rights. Click Next.
7. Supply the password for the local administrator and a username that must be added to the Local Administrators group. Click Next.
8. Select the target drive that needs to be captured and where the new operating system needs to be installed, and click Next.

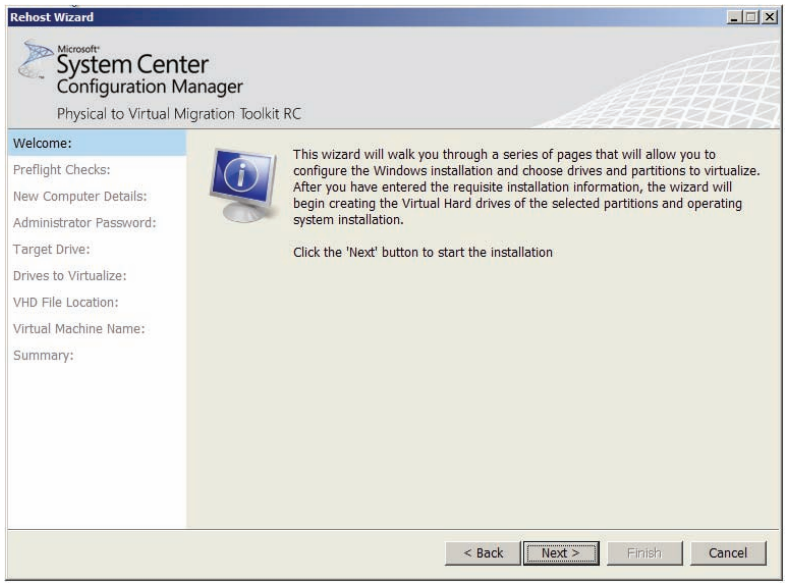


Figure 3.24
The Physical to Virtual Migration Toolkit

9. Select the drives to virtualize, and click Next.
10. Supply a UNC path to a location where the new virtual hard disk (VHD) image can be saved.
11. Supply the credentials of a user who will have permissions to save to the virtual hard drive.
12. Click Next.
13. Supply a new name for the virtual machine, the memory, the virtual network name, and the network that will be connected to the virtual machine. Click Next to continue.
14. After reviewing the Summary screen, click Finish, and the process will start.

The task sequence will begin the physical-to-virtual process. Once that is complete, the operating system will be installed and the VHD files will be added to Hyper-V on the new operating system.

Creating Non-Task-Sequence Bootable Media

Another option is to create non-task-sequence bootable media; this can also be a CD/DVD set or a USB flash drive. This procedure is just to create a virtual hard disk that can be used in Hyper-V. Non-task-sequence bootable media is created with the following procedures.

To create a stand-alone media USB flash drive, do the following:

1. Start the P2V Migration Toolkit.
2. Select Create Windows PE Boot Media. In the next screen of the WinPE Creator Wizard, select the boot image OS architecture type to target in order to create the bootable Windows PE image, and then click Next.
3. Select USB Flash Drive, as shown in Figure 3.25 and click Next.

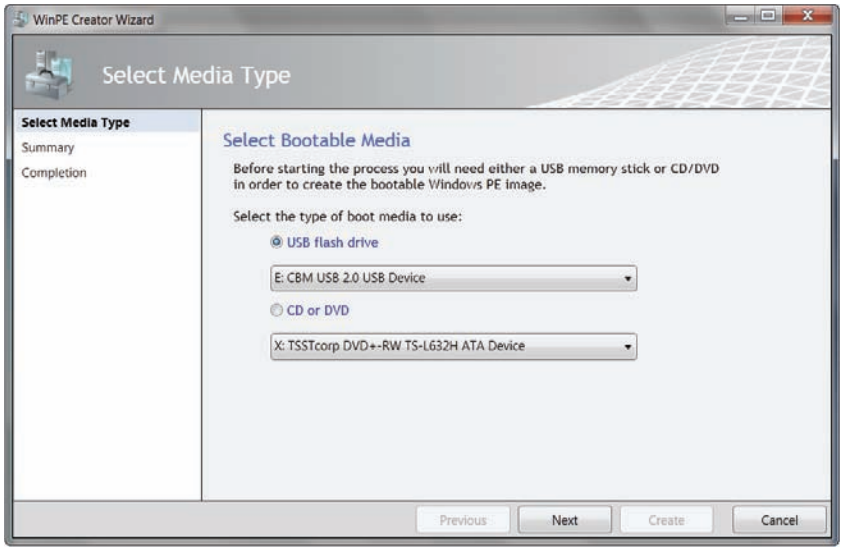


FIGURE 3.25
Selecting the USB flash drive

4. Click Yes if you want to format the USB flash drive, and click Next.
5. Review the Summary screen, and click Create.
6. When the wizard has completed successfully, click Close.

To create a stand-alone media CD/DVD set, perform these steps:

1. Start the P2V Migration Toolkit.
2. Select Create Non-Task Sequence Bootable Media.
3. Select CD or DVD, select the CD/DVD drive with an empty CD or DVD, and click Next.
4. Review the Summary screen, and click Create.
5. When the wizard has completed successfully, click Close.

After creating the stand-alone media USB device or DVD/CDs, you can boot the Configuration Manager 2007 site server from that media and start the following process:

1. Boot the branch office site server from either USB or CD/DVD.
2. Click Next on the Welcome page of the bootable device.
3. Select the drives to virtualize, and click Next.
4. Supply a local path to a location where the new virtual hard disk (vhd) image can be saved. This can be a USB disk. Click Next.

   The file is created and copied to the defined location.
5. Once the creation is complete, click Finish.

When it has finished, copy the VHD image to a Windows Server 2008 R2 server and configure a virtual machine in Hyper-V to use the VHD image.



Real World Scenario

Migrating to Configuration Manager 2012

Sports Clothes United Inc. develops and sells sports clothing to retailers and their own shops all over the world. The head office is located in San Francisco. The company is growing so fast that they acquire a new company called Fit Clothes. Fit Clothes has their own Configuration Manager 2007 R3 SP2 environment.

You as a consultant or Configuration Manager administrator are asked to migrate the Fit Clothes Configuration Manager 2007 R2 SP2 environment to the new Configuration Manager 2012 infrastructure and deploy the corporate standard of Sports Clothes United.

Migration Scope

The corporate IT department investigated the Configuration Manager 2007 R3 SP2 environment of Fit Clothes and came to the conclusion that only the classic packages, advertisements, and collections need to be migrated to the Configuration Manager 2012 environment of Sport Clothes United. After the classic packages are migrated, they must be converted to the new application model.

Your assignment is to migrate these assets.

Migration Approach

Because the corporate IT department decided that the assets need to be migrated, you must use the migration feature of Configuration Manager 2012. You always need to test your migration approach in your test lab and define and crystallize your steps while testing your approach. The following steps should be used:

1. Define the topmost source site as the source hierarchy.
2. Configure credentials to be able to gather data from the source site(s).
3. Use the collection migration to migrate your collections with the associated applications and advertisements.
4. After successfully migrating the classic packages to Configuration Manager, analyze the packages to discover the readiness level for the new application model.
5. Convert the classic packages with a readiness level of Automatic.
6. Fix and convert the packages with a readiness level of Manual.
7. Stop the data-gathering process, and clean up the migration data.
8. Uninstall Configuration Manager 2007.

Once you have completed those steps, you will have migrated the required Configuration Manager 2007 assets to Configuration Manager 2012.

The Bottom Line

Determine what you are able to migrate with the migration feature. The new migration feature in Configuration Manager 2012 allows you to migrate the old Configuration Manager investments to Configuration Manager 2012 side by side. In earlier versions you were able to migrate the server in place or side by side by replicating data, but no real manageable migration feature was available.

Master It With the migration feature you cannot migrate things like the following:

- Queries
- Security rights for the site and objects
- Configuration Manager reports from SQL Server Reporting Services
- Configuration Manager 2007 web reports
- Client inventory and history data
- AMT client-provisioning information
- Files in the client cache

To keep it positive, identify what objects you are able to migrate with the migration feature of Configuration Manager 2012.

Discover which migration approach is supported. Configuration Manager 2012 provides migration features that can be used for your migration of Configuration Manager 2007 to Configuration Manager 2012.

Master It With the earlier upgrades or migrations of Configuration Manager in your mind, what migration approaches are supported when migrating from Configuration Manager 2007 to Configuration Manager 2012?

Ascertain what kind of interoperability is supported during the migration. Interoperability like that supported in earlier versions is no longer supported; nevertheless, the migration feature of Configuration Manager 2012 supports some kinds of interoperability during the migration process. Depending on the size of your Configuration Manager 2007 or Configuration Manager 2012 source hierarchy, the migration can take some time.

Master It Interoperability like you were used to in SMS 2003 and Configuration Manager 2007 is no longer supported. Give two examples of interoperability features in Configuration Manager 2012.

Migrate packages and programs to the new application model. The classic packages just migrated to Configuration Manager 2012 can be used and targeted to collections of users and computers, but Configuration Manager is built around a new application model that allows you to implement user-centricity in your Configuration Manager 2012 environment.

Master It Converting classic packages to the application model is not a feature of Configuration Manager, but with extra software it can be done from the Configuration Manager 2012 console in a couple of different ways. What is the name of the tool that you use to convert the classic packages, and what are the steps to convert a classic package?



Chapter 4

Installation and Site Role Configuration

Previous chapters have already begun pulling back the covers on the changes in Configuration Manager 2012 R2. This chapter is focused on discussing Configuration Manager 2012 R2 sites, hierarchies, and site system roles and provides a walkthrough of building a sample hierarchy.

A major design pillar for Configuration Manager 2012 R2 was hierarchy simplification. In previous versions of Configuration Manager it was not uncommon to find hierarchies with dozens of sites and, in some cases, thousands of sites, and often hierarchies would be built four to five or more layers deep. Both the number of sites in a hierarchy and the depth of the hierarchy bring with them configuration complexity, potential delays, and sometimes errors when transmitting data from the top level of the hierarchy to the bottom tier sites.

Configuration Manager 2012 R2 changes potential hierarchy design significantly in a few ways. Because of the numerous changes and efficiencies—not the least of which is enhancements in the security model—in many cases, organizations with fewer than 100,000 client systems won't need to implement a hierarchy at all. A single site server and its associated "helper" servers will be all that is necessary to provide a robust Configuration Manager 2012 R2 experience.

A hierarchy will be required by organizations that manage more than 100,000 clients or have other nontechnical reasons that require a hierarchy to be implemented, such as legal or political requirements. In those cases, the efficiencies gained in Configuration Manager 2012 R2 should often result in far fewer numbers of installed sites and, as a result, a simpler hierarchy.

A couple of interesting facts about hierarchy changes in Configuration Manager 2012 R2 will serve to whet your appetite for what is to come. A Configuration Manager 2012 R2 hierarchy supports only a single tier of primary sites. A tier of secondary sites may be added if absolutely necessary, but in most cases, as detailed in the chapter, there is no reason for secondary sites any longer.

In this chapter, you will learn to

- Understand Configuration Manager 2012 R2 sites and the new approach to hierarchy design
- Construct a Configuration Manager 2012 R2 hierarchy
- Determine when to expand a hierarchy and when to simply add a site system role for additional service
- Deploy and configure the various site system roles available per site

Understanding Configuration Manager 2012 R2 Site Types

It doesn't take long when working with any of the versions of Systems Management Server or Configuration Manager to be introduced to the concept of a site server. Site servers exist to provide service to Configuration Manager clients. Site servers understand which clients they should serve by defining management boundaries, which may be AD sites, IP subnets, or IP address ranges. Depending on the size and organization of the Configuration Manager environment, there may be a need to have more than a single site to manage all of the clients in the enterprise. When more than one site is needed, it is common to establish a site hierarchy, which will facilitate centralized management of all Configuration Manager clients.

A specific design goal of Configuration Manager 2012 R2 is to reduce the number of sites that are needed in a hierarchy and also to reduce complexity. Further discussion of this will come shortly.

Site servers historically have fallen into one of two categories, either a *primary site server* or a *secondary site server*, and now a third type is part of Configuration Manager 2012 R2, the *Central Administration Site (CAS)*.

Primary Site Server A primary site server has historically been identified as having a few characteristics:

- It has its own database hosted on SQL Server to maintain configurations.
- It is the only site type where clients can be directly assigned.
- It has the ability to host child sites—either other primary sites or secondary sites.

Both the first and last characteristics are no longer items that distinguish a primary site. In Configuration Manager 2012 R2 primary site servers *do* still have their own copy of SQL running, but secondary sites do as well. Further, a primary site *can* have child sites, but those child sites can *only* be secondary sites. Introduced in Configuration Manager 2012 R2 is the fact that only primary sites can be assigned to the Central Administration Site—secondaries need not apply!

Secondary Site Server A secondary site server has historically been identified by a few characteristics:

- It does not make use of a SQL database.
- There is no way to directly administer a secondary site; all administration would have to come from an administration console connected to a primary site somewhere above the secondary.

The former condition is no longer true—secondary sites now *do* have a database. When installing a secondary site, you have a choice of either using an existing instance of SQL or, if SQL is not present on the target server, installing and using SQL Express. The latter observation remains true—secondary sites cannot be administered directly through the console.

Also, the historical justification for secondary sites has primarily been to provide local content access for clients residing in or roaming into its defined boundaries and to help control network traffic for content moving between the secondary site and its assigned parent primary site. Secondary sites are still used for that purpose today (although the argument is far less compelling).

So, secondary sites still are available in Configuration Manager 2012 R2, but before you plan to install one, check out the various bandwidth-control features of Configuration Manager 2012 R2. One key addition is that it is now possible to control, or throttle, network bandwidth between a site and its remote distribution points within the site. This one addition in Configuration Manager 2012 R2 makes it at least worth considering whether secondary sites really are necessary. If secondary sites were in use in an environment for the sole purpose of controlling network bandwidth for content distribution (some content is *huge*), then the ability to throttle content delivery between a site and a remote distribution point introduced in Configuration Manager 2012 R2 will be of interest. We'll cover this shortly.

Other reasons for having a secondary site include the ability to throttle non-content site-to-site communications. This is a much reduced data size compared to content, but if throttling is still of concern to you, then a secondary site may be justified. (In previous versions of Configuration Manager this content would be files that contained status information, site configuration information, client information, and so on. In Configuration Manager 2012 R2 this content is still transferred between sites but is split between traditional file-based transfer and SQL replication.)

When it comes to secondary sites—or any other site type for that matter—*think* before following the same old pattern for a hierarchy. Configuration Manager 2012 R2 is about hierarchy simplification after all and really does a nice job of increasing site efficiency!

Central Administration Site Another type of site that has been around in previous versions of ConfigMgr is the central site server. A central site server is the one at the top of a hierarchy and is used to centrally administer the entire Configuration Manager implementation. Because of its role in hierarchy-wide management, a central site typically should not have clients directly assigned (although it is possible). Further, because all information in the hierarchy resides at the central site, this is typically the key site in the hierarchy where reporting is configured.

The central site server is no longer present in Configuration Manager 2012 R2. It has been replaced by a new type of site server known as a Central Administration Site (CAS). The CAS is much like the central site server except that it cannot have any clients assigned (not even an option), some site functions are not available at the CAS (such as most of the discovery options), and the CAS must be installed as the first site of the hierarchy. However, if you decide not to install the CAS until your organization has reached a desired limit of clients, you can expand your stand-alone primary site into a CAS only one time.

As we mentioned, sites manage clients. To facilitate client management and depending on the services being delivered, several different functional roles must be in place at the site. These functional roles are either added to the site server itself or configured on external servers. Either way, the servers that host these support roles are known as site systems. The option for distributed site servers to fulfill various functions allows for very flexible and scalable designs. Ultimately, the decision on where to place these site systems or whether to use external site systems at all is up to the administrator. And, if these roles need to be moved to other servers after installation, or other servers need to be added, that is easy to do. This work is performed in the Administration workspace, under Site Configuration of the Configuration Manager console, as shown in Figure 4.1.

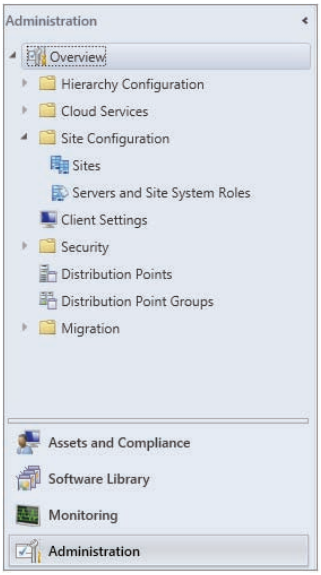


Figure 4.1
The Administration workspace within the Configuration Manager 2012 R2 console



Real World Scenario

Hierarchy Design and Implementation

Now that we've discussed the types of sites available in Configuration Manager 2012 R2, it's natural to begin thinking about implementation details. Hopefully it is clear that Configuration Manager 2012 R2 introduces significant changes in terms of site and hierarchy design. Administrators who have experience with previous versions of Configuration Manager might be tempted to set up Configuration Manager 2012 R2 in the same design that is currently being used. That approach might work, but it would be a mistake and would likely mask many of the features for simplified management that are available in Configuration Manager 2012 R2.

One of the major design pillars for Configuration Manager 2012 R2 was hierarchy simplification. With that in mind, during the design phase remember that each primary site is capable of supporting 100,000 client systems, and the hierarchy as a whole is able to support 400,000 clients. This means that for many organizations the total Configuration Manager 2012 R2 design might be handled with only a single primary site along with additional servers to support various roles in the environment. It's interesting to note that even in Configuration Manager 2007 a primary site was also able to support 100,000 clients. That type of scale often was not realized because of the need for additional sites for political or load reasons. The design of Configuration Manager 2012 R2 removes virtually all technical reasons for adding additional site servers unless the addition is driven by scale.

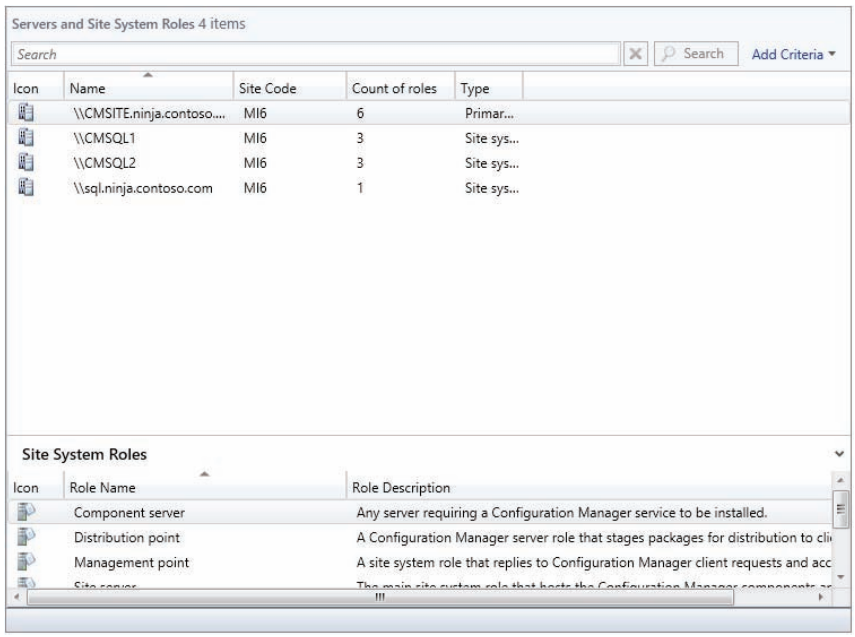
Implementing Site Servers

The terms *site* and *site server* are often used interchangeably. In reality this shouldn't be the case. A Configuration Manager 2012 R2 site encompasses all servers that are used to deliver the services offered by the site. Said another way, a Configuration Manager 2012 R2 site can consist of one to several servers. The size of the site will dictate how many servers are needed to deliver service to clients. In smaller environments it may be that only a single server is needed to host all components needed to deliver the site's services. In larger environments multiple servers may be needed. With the new design of Configuration Manager 2012 R2 the expectation is that the number of total sites needed for an environment will decrease, but the number of supporting servers for a site might increase.

A site server is the one server in a site that orchestrates delivery of service to clients. This server will interact with any other servers that are in place supporting the site's ability to deliver services. These additional servers are known as site systems. (A site server is also a *site system*.)

As services are added to a site and assigned to a server, the list of site system roles will increase. A quick glance at the Configuration Manager console will reveal the site systems that are in use to support a site and also what services those site systems are delivering on behalf of the site. An example is shown in Figure 4.2. Note that two systems are shown related to site code PRI. One is the site server itself and the other is a site system server providing service for the site.

FIGURE 4.2 Site systems and roles



Software Requirements

Before further discussing Configuration Manager 2012 R2 it is beneficial to install the software. There are a few prerequisites for installing a site server. For a full list of these prerequisites, go to

```
http://technet.microsoft.com/en-us/library/gg682077.aspx
```

These prerequisites may also apply to site systems that may be installed, depending on the services, those servers will offer:

- All site servers must be members of a Windows Active Directory domain (Windows Server 2003 functional level or above if using the discovery filter for stale computer records).
- The site servers must be deployed on 64-bit hardware. Configuration Manager 2012 R2 is a native 64-bit application, and there is no version that can be installed on 32-bit systems. (32-bit systems are supported as Configuration Manager clients and some site systems.)
- .NET Framework 3.5 SP1 and 4.0 must be installed.
- Microsoft XML Core Services 6.0 or greater must be installed.
- Microsoft Remote Differential Compression must be installed.
- SQL Server 2008, 2008 R2, or 2012 is required to host the ConfigMgr database.

And don't worry; if a required configuration happens to be missed along the way, the Configuration Manager 2012 R2 prerequisite checker, which runs as part of the install wizard, will let you know. The details of the checks that are performed during prerequisite validation are recorded in the `ConfigMgrPrereq.log`, located in the root of the `C:` drive of the server where Configuration Manager 2012 R2 is being installed. If it would be helpful to run the prerequisite checker outside of the Configuration Manager 2012 R2 setup wizard, it is available as a separate executable located in the `\SMSSETUP\BIN\`*`X64`* folder of the installation media. The filename is `PREREQCHK.EXE`. The following list documents the prerequisite checks that are done as part of the install or as part of independently running the Prerequisite Wizard. The list of prerequisite checks is detailed for the Central Administration Site. Any additional checks performed are detailed for other site types.

Central Administration Site

- Confirm targeted server is a Windows server.
- Confirm operating system is a supported version.
- Verify targeted server is a domain member.
- Check to ensure schema extension has been completed and is correct.
- Confirm disk space is sufficient for installation.
- Confirm disk size for installation.
- Verify MSXML 6.0 is installed.
- Verify Remote Differential Compression is installed.
- Confirm the correct version of MSI is installed.
- Confirm .NET Framework Version 3.5 is installed.
- Verify SQL SysAdmin rights are configured.

- Verify site server computer account has administrative rights.
- Confirm SQL Server security mode.
- Verify SQL Agent logon.
- Confirm version of SQL Server is as required.
- Verify firewall settings for SQL Server access.
- Confirm SQL Server is configured as not case sensitive.
- Verify connectivity to SQL Server.
- Confirm WIM filter driver is installed.
- Verify sufficient disk space for installing the Windows Automated Installation Kit.
- Confirm ConfigMgr is not already installed.
- Verify sufficient disk space for SDK server.

Primary Site

- Confirm the user installing the primary site has administrative rights on site system and CAS (if applicable).
- Verify connectivity to CAS (if applicable).
- Confirm disk is *not* formatted with FAT partition.
- Check to see if WSUS is installed on the site server and, if so, whether it is of the proper version.
- Verify Windows Server 2003 SChannel hotfix is installed.
- Verify Windows Remote Management 1.1 is installed.
- Confirm MMC updates are installed.
- Confirm .NET update for Configuration Manager is installed.
- Verify PowerShell 2.0 is installed on the site server.

Some prerequisite checks may trigger a warning, but if they aren't critical for a successful site installation, the installation process is allowed to proceed.

Implementing a Central Administration Site

Installing Configuration Manager 2012 R2 begins by installing the first site. A very important question should be answered before launching the Setup Wizard: Is it expected that more than a single primary site will need to be included in the deployment? If the answer is *yes*, then the very first site that needs to be installed is the Central Administration Site. The CAS is the top site in the hierarchy and is used solely for administration of the entire hierarchy. No clients or client-related functions are possible at the CAS. This is critical to understand. If there is any expectation of joining multiple primary sites in a hierarchy relationship, then the CAS must be the first server installed. If it's not installed, then you should plan to expand the stand-alone site to a CAS at a later time.

For those of you who have worked with previous versions of Configuration Manager, your initial reaction may be that multiple sites *are* needed because they were needed in the current implementation (whatever version that is) of Configuration Manager. Not so fast! Remember that one of the design goals of Configuration Manager 2012 R2 is hierarchy simplification. A Configuration Manager 2012 R2 site is more efficient in many ways, not the least of which is the ability to throttle traffic to remote distribution points (thus often eliminating the need for secondary sites). This one tweak by itself will go a long way to reducing the number of sites. Further, a single site has been able to scale to support 100,000 clients for some time now. Often, this kind of scale for a single site was not realized because of the need for additional sites due to network conditions, security considerations, and the like. With Configuration Manager 2012 R2 and hierarchy simplification along with other improvements, expect to see primaries carrying much more of a client load than might have been seen in previous versions.

For the examples given here, installation will proceed assuming a three-site hierarchy is to be built. The hierarchy will consist of a single CAS, a single primary site, and a single secondary site.

With the decision made as to how many sites are needed for the hierarchy, the first site to be installed is the CAS. Before starting the Setup Wizard, make sure SQL is installed and available. Also, install the Windows Assessment and Deployment Kit for Windows 8.1 first (it's required).



Real World Scenario

Choosing Local or Remote Installation

A SQL Server installation can be either local or remote. Arguments rage about the best approach. This argument is helped in Configuration Manager 2012 R2 by some support boundaries. A single primary site server on appropriate hardware is able to support 100,000 clients, but if SQL is collocated with the ConfigMgr application, that same primary site server is supported for only up to 50,000 clients. This is mostly due to the load that SQL replication introduces. Still, while the performance differences between a remote versus local SQL server when properly configured are slight, if a site will host fewer than 50,000 clients, using collocated SQL is still preferred and is considered most efficient. One reason for this is that when SQL is running on the same system, it is possible to take advantage of the shared memory protocol. One consideration for local SQL, however, is the default memory settings. SQL by default is configured to consume all available RAM. This is a good configuration for standalone SQL because RAM is more efficient than disk memory.

When sharing a server, setting a maximum amount of RAM for SQL consumption and thereby reserving the rest for Configuration Manager, the operating system, and other applications such as virus scanners is an optimal configuration. SQL does a very good job of managing RAM and not over-consuming and starving other applications, but there is a cost, however slight, because SQL pages information out of RAM to make room for the needs of other applications. Setting a maximum from the beginning avoids this problem, and with the amount of RAM available on servers today, there really shouldn't be an issue with specifying a maximum RAM value for SQL.

Finally, it's time for installation! The installation process is wizard driven and does a good job of keeping you on track. The most difficult part of the installation is knowing what options to choose. The example will explain how to configure the various options and what they mean. Let's get started:

1. Insert the installation media, and autorun should cause the initial installation screen to be displayed.

   If this is not the case, or if you're running from a location other than the supplied media, simply double-click the `splash.hta` file, which will display the initial installation screen.

   The splash screen provides options for accessing various documentation and assistance, even links to the Configuration Manager community. There are also links to access server readiness components and links to download Configuration Manager updates that are required during the installation process. These latter links are really nice additions to Configuration Manager 2012 R2, providing a very easy way to download updates and move them to a server that is being installed that may not have Internet access to download the updates during setup. Other links include options to just install the Configuration Manager 2012 R2 console and to download System Center Updates Publisher—a tool that anyone using software updates should take a look at! Clicking the Install link at the top left of the screen launches the Setup Wizard and opens the Setup Wizard Welcome page.

2. Review the information on the Before You Begin page, and click Next to continue to the Getting Started page.

   On the Getting Started page the various install options are presented. The options available here will be based on the state of the system where the install is being run. If a system already has Configuration Manager 2012 R2 installed, only the options to uninstall or perform a site reset may be available. If you're running the wizard on a system without Configuration Manager 2012 R2, the options will be as shown in Figure 4.3.



FIGURE 4.3
Setup Wizard: Getting Started page, when installing on a system without ConfigMgr

This is the point in the wizard where the decision you made earlier is configured—whether to install a stand-alone primary site or to install a Central Administration Site. This installation will be for a Central Administration Site.

3. With that option selected, click Next to continue to the Product Key page. Decide whether to install as an evaluation or to supply a product key. Once you've entered the key, click Next to continue to the Microsoft Software License Terms page.

4. On the Microsoft Software License Terms page, review the information. If you agree, select I Accept These License Terms and click Next to proceed to the Prerequisite Licenses page.

5. On the Prerequisite Licenses page, review the information. This page requires you to accept the license terms for SQL Server 2012 Express, SQL Server 2012 Native Client, and Microsoft Silverlight 5. If you agree, select the appropriate box to accept the terms for each, and click Next to proceed to the Prerequisite Downloads page, shown in Figure 4.4.

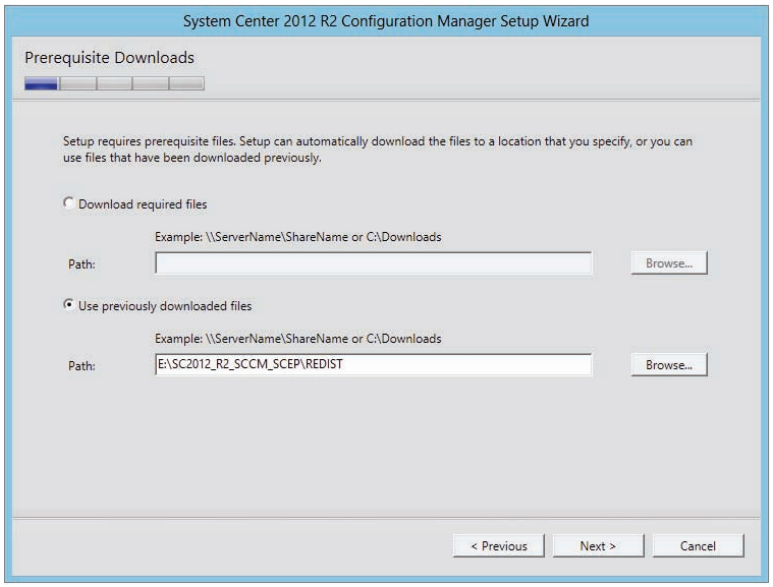


FIGURE 4.4
Setup Wizard: Prerequisite Downloads page

6. On the Prerequisite Downloads page, decide whether to download the updates or, if the updates have been previously downloaded—either from another site installation or using the link on the initial splash page—select the second option.

   In both cases, a path for the updates should be specified. For the example, the updates have been previously downloaded and will be installed from the path shown.

7. Once you've completed this screen, click Next, which, depending on the selection made, will initiate the update download process or update evaluation. Once this step is complete, the wizard moves on to the Server Language Selection page.

When migrating from a previous version of Configuration Manager to Configuration Manager 2012 R2, it might be useful to have both consoles installed on a system. Doing so is fully supported.

8. Choose the languages you want to support. The default is English. Once you've completed this screen, click Next to go to the Client Language Selection page. On the Client Language Selection page configure additional languages that should be supported from a client perspective. The default here is English. Once you've done this, click Next to proceed to the Site and Installation Settings page, shown in Figure 4.5.

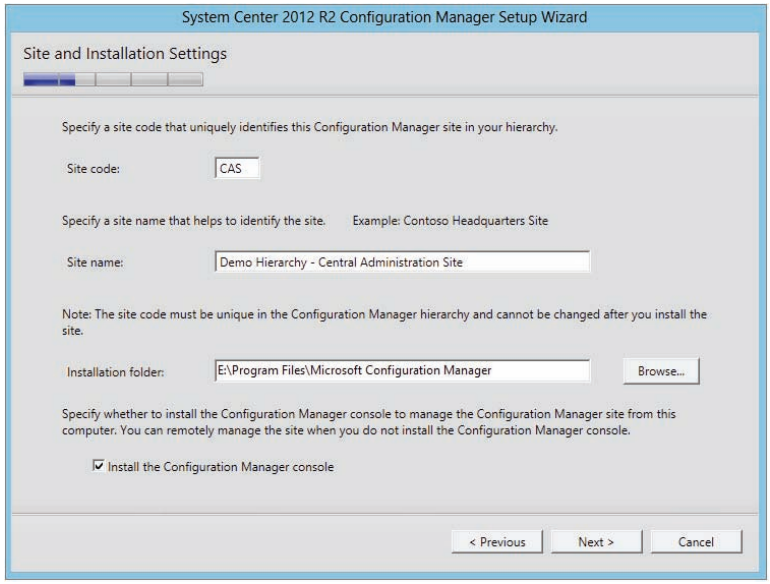


Figure 4.5
Setup Wizard: Site and Installation Settings page

On the Site and Installation Settings page several options are available. The first required option is the Site Code field. The site code can be any three-character alphanumeric code but cannot contain any special character such as a dash or ampersand. In fact, to ensure no mistake is made here, the wizard won't even accept special characters for the site code. Next is the Site Name field. Choose a descriptive name and enter it into this box. Finally, input the installation path where ConfigMgr should be installed.

Setting the correct path is a critical part of installing Configuration Manager 2012 R2. The default path is on the `C:` drive, and for the example, we will use the `E:` drive for best practice.

Selecting a Disk for Installation

In production environments it is not recommended to install Configuration Manager on a disk shared by other disk-intensive applications, including the operating system, SQL databases, or the page file. Doing so may degrade Configuration Manager performance.

The last option is a choice of whether to include the Configuration Manager 2012 R2 console as part of the installation. This option is commonly used and is checked by default. If you don't want this option, remove the check mark. If you need the administrative console at a later time, you can easily add it.

9. Click Next to proceed to the Database Information page, as shown in Figure 4.6.

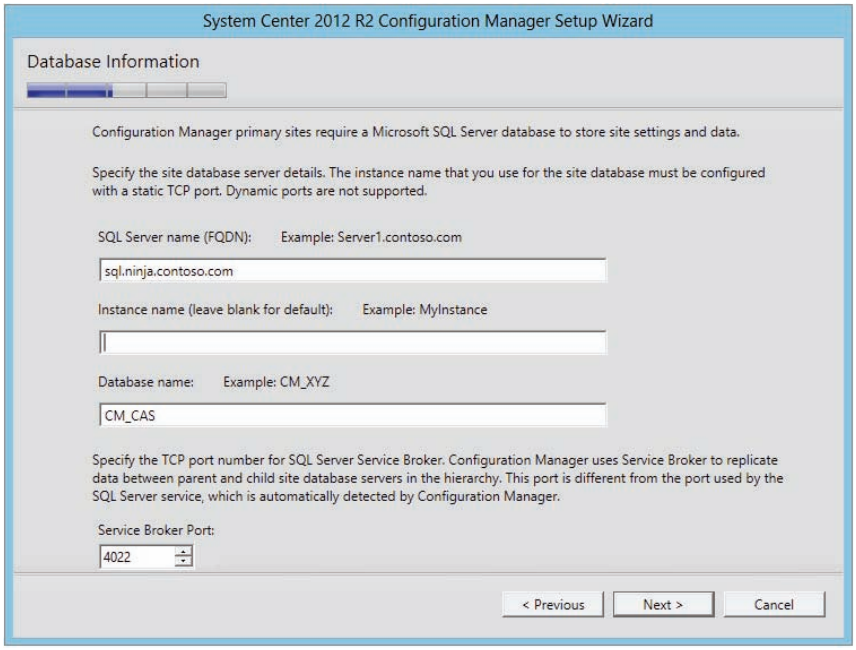


FIGURE 4.6 Setup Wizard: Database Information page

10. On the Database Information page configure the SQL Server information.

    For the example, SQL is installed on the same server where the Setup Wizard is being run, so the default location that shows up for SQL Server is the local server. If you're installing SQL on a remote server, enter the name of that remote server in the SQL Server Name box.

    An option to name the database is also provided. If a different database name is preferred, modify the default entry as needed.

11. Click Next to proceed to the SMS Provider Settings page, where an option is given to specify where the SMS Provider should be installed.

    You may ask, what is the SMS Provider? Detailed information on the SMS Provider can be found at

    `http://technet.microsoft.com/en-us/library/bb680613.aspx`

But in short, the SMS Provider is the resource the Configuration Manager 2012 R2 console uses for most of its access to data residing in the Configuration Manager 2012 R2 database.

In the example, the Central Administration Site and SQL are installed on the same server, so it only makes sense that the SMS Provider be collocated on that same server. If the SQL Server being used for the Central Administration Site were remote, then you'd need to choose whether to place the SMS Provider on the Central Administration Site or on the SQL Server. Typically the provider would be placed on the SQL Server in that configuration for best performance. It is also possible that the SMS Provider could be placed on a totally separate server. In practice, it is an uncommon condition where using a separate server to host the SMS Provider is warranted. More information regarding SMS Provider placement is available in the "About SMS Provider Locations" section of the "Planning for Site Systems in Configuration Manager" document available at

`http://technet.microsoft.com/en-us/library/gg712282.aspx`

12. Configure the location, and then click Next to proceed to the Customer Experience Improvement Program page. Review the information and decide whether to participate in the program.
13. With the selection made, click Next to proceed to the Settings Summary page, as shown in Figure 4.7.

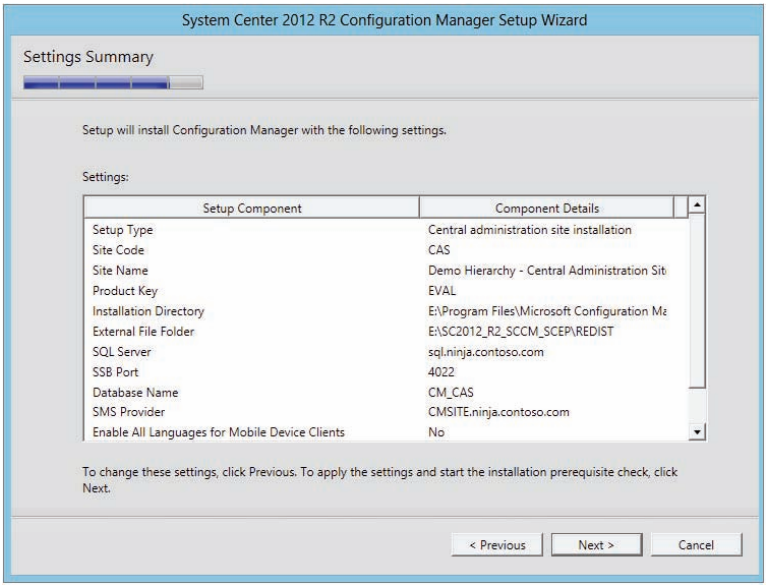


FIGURE 4.7 Setup Wizard: Settings Summary page

14. On the Setting Summary page, review the configured settings, and if corrections are needed, use the Previous button to move backward in the wizard and correct any mistakes.

15. Once all settings are as desired, click Next to proceed to the Prerequisite Check page, shown in Figure 4.8.

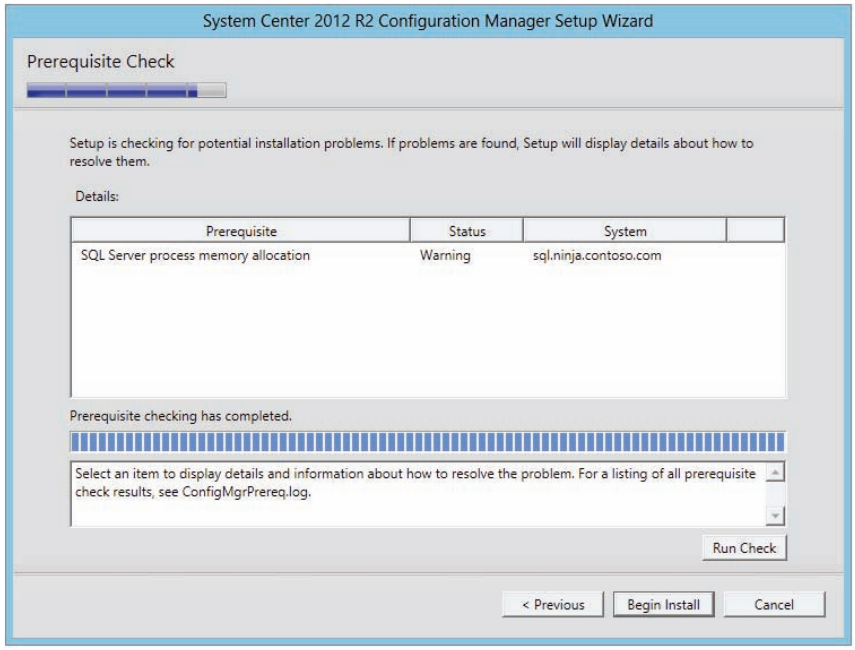


FIGURE 4.8 Setup Wizard: Prerequisite Check page

On the Prerequisite Check page, the wizard immediately starts the Prerequisite Wizard to verify that all components required for a successful installation are present. Note that in the figure one item is flagged with a Warning status. Missing prerequisites that are not vital to successful installation will be listed with a warning to raise awareness of their absence. Common warning conditions listed are as follows:

Schema Extensions This warning alerts administrators to the possibility that Active Directory schema extensions may not be installed. In most cases, extending the Active Directory schema is advantageous, but in some corner cases it can cause confusion.

WSUS SDK On Site Server This warning alerts administrators to the fact that there is no installation of Windows Server Update Services (WSUS) on the CAS. In most environments ConfigMgr is used to deploy software updates. Software update functionality requires WSUS components to be installed. When they aren't, the warning results.

AD Permissions In order to publish to Active Directory the site server must have permissions. This warning is an alert to administrators that required permissions may not be in place.

SQL Memory Usage By default SQL server is configured to consume all available memory and to manage the memory so that other applications have what they need and SQL has the rest. While good in theory, and where a server is dedicated to SQL, when other enterprise applications share a system, which is the case when ConfigMgr is collocated with SQL server, there can be some performance degradation due to memory management. It is recommended in such cases to place a maximum on the amount of memory available to SQL. This is done directly in the SQL interface.

SQL Server Process Memory Allocation This warning alerts administrators that on the CAS it is recommended that SQL Server be allocated no less than 8 GB of memory.

Having the listed components installed may or may not be appropriate for a specific scenario depending on the ultimate configuration of the server. If only warning messages are listed, then it is OK to proceed with the install. These warning scenarios can be fixed later if need be. If any critical prerequisites are missing, then setup cannot proceed.

16. Fix anything that shows a Critical status, and run the prerequisite check again by clicking Run Check. If more information is needed about a particular prerequisite, click any specific item to see more detail.
17. Once all prerequisite issues are resolved, click Begin Install to proceed to the Install page and begin installation. Figure 4.9 shows the page after installation is finished.

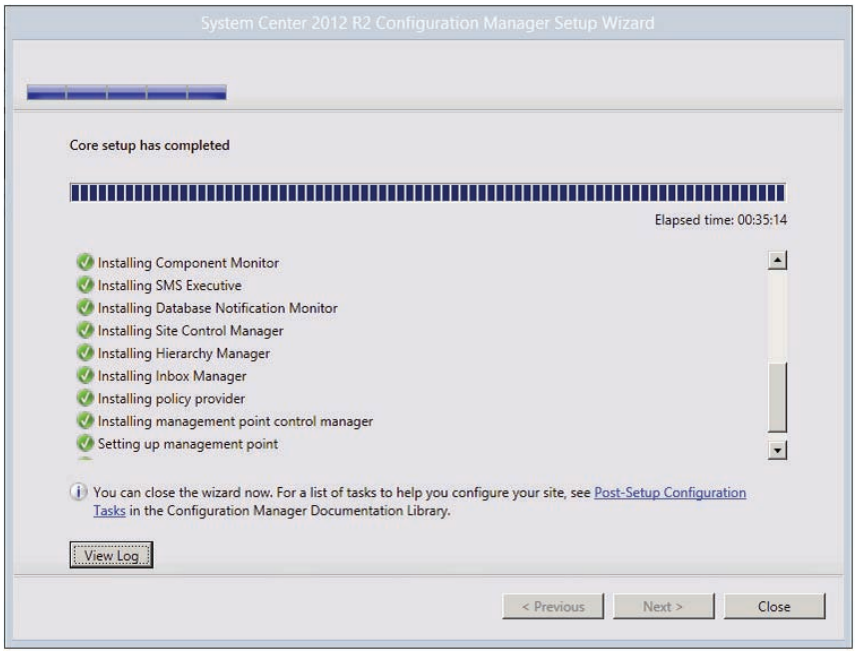


FIGURE 4.9
Setup Wizard: Install page: installation complete

The wizard will remain on the same page, and each phase of the installation will be listed, along with its status, as the installation proceeds. Depending on hardware the installation will take several minutes or longer. One of the longest steps is installing the boot image package used for operating system deployment.

18. Once the install completes, scroll through the list of installed components, verifying that each has completed successfully.

19. Also, review the details of the installation procedure by clicking View Log.

    The setup process is recorded in two logs, the `ConfigMgrSetup.log` and the `ConfigMgrPrereq.log`. If you're installing the administrative console, that portion will be recorded in the `ConfigMgr AdminUISetup.log`. Lastly, the wizard progress is recorded in the `ConfigMgrSetupWizard.log`. All of these logs are located in the root of the `C:` drive where ConfigMgr was installed.

20. When you're ready, click Close to exit the wizard.

And that's it; the Central Administration Site is now installed. Feel free to explore the console at this stage if you like. The next step is to install a primary child site and attach it to the Central Administration Site. Proceed to the next section when ready.

Implementing a Primary Site

The next step in building out a hierarchy is to install a primary site. Remember that primary sites can exist either stand-alone or in association with other sites in a structure known as the site hierarchy. As a reminder, if you're installing a primary site in a stand-alone configuration, it can never be joined to a CAS without a reinstall. If you're planning a primary site as part of a hierarchy, which is the case for our example, that primary site must be installed and joined to the Central Administration Site. Said another way, a primary site in Configuration Manager 2012 R2 must be a child site of the Central Administration Site. This implies that there can be only a single tier of primary sites in the hierarchy. That implication is correct. Unlike previous versions of Configuration Manager, where it was possible to build hierarchies multiple layers deep with primary sites, Configuration Manager 2012 R2 allows only a single tier of primary sites. This change was made specifically to help simplify hierarchies and increase the efficiency and speed of data moving from one site to another. With Configuration Manager 2012 R2, it is possible to have up to four tiers of hierarchy if secondary sites are used. More on that soon, but for now, let's install the primary child.

The Setup Wizard is very similar when installing a primary child site. There really are only a few differences. Since we've already discussed the setup process for a Central Administration Site, we'll examine only the specific steps that are different for installing a primary site.

1. As before, ensure that the server where the primary site will be installed meets all prerequisites and is ready to receive the installation.

2. When you're ready, launch the splash page, choose to install, and move through the wizard using the information we've already discussed until arriving at the Getting Started page, accept the license agreement and continue until it show available setup options as shown in Figure 4.10.

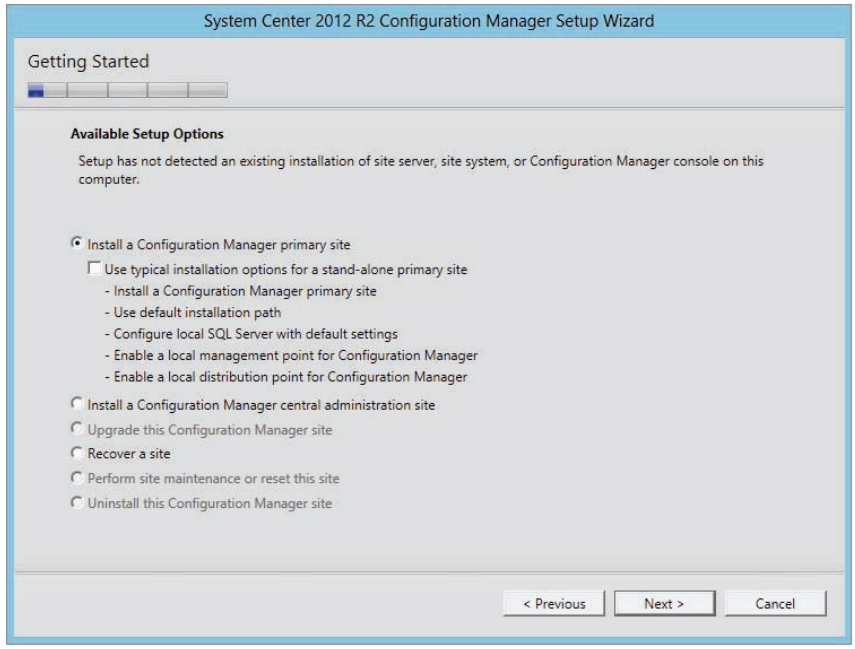


Figure 4.10
Setup Wizard: Getting Started page for a primary site

Installing Stand-alone vs. Inclusion in a Hierarchy

If you're installing a stand-alone primary site and if the option Use Typical Installation Options For A Single Server Installation is selected, then certain pages of the Setup Wizard will be skipped, including the ability to change the directory in which Configuration Manager is installed. This option would be similar to the simple install option available with Configuration Manager 2007. While this option exists, my experience is that most Configuration Manager administrators prefer to see each option as the wizard proceeds to ensure nothing is configured in error.

It is possible to select the option Use Typical Installation Options For A Single Server Installation even when the intent is to join the new primary site to a hierarchy. At this stage of the installation process, setup doesn't have sufficient information to know the intent. If the option is selected, there will be no option to join to a Central Administration server.

This is the first place where the setup process will differ from what has already been described.

3. On this page, ensure that the option Install A Configuration Manager Primary Site is selected, but do *not* choose Use Typical Installation Options For A Single Server Installation because this installation isn't for a stand-alone primary site. Click Next, and proceed through the wizard as before until arriving at the Prerequisite Components page.

4. On the Updated Prerequisite Components page, select the option Use Previously Downloaded Updates From The Following Location, and specify the update folder used when installing the Central Administration Site.

   Since the updates are already downloaded and local, this setting should prevent any download delays. Click Next to continue.

5. Continue through the wizard until arriving at the Primary Site Installation page. There, you can choose to install the primary site in a stand-alone configuration or join it to the Central Administration Site.

6. The example installation is to be part of a hierarchy, so do the following:

   a. Select the Primary Site Will Be Joined To An Existing Hierarchy option.

   b. Specify the name of the Central Administration Site server.

   c. Click Next to proceed to the Database Information page, shown in Figure 4.11.

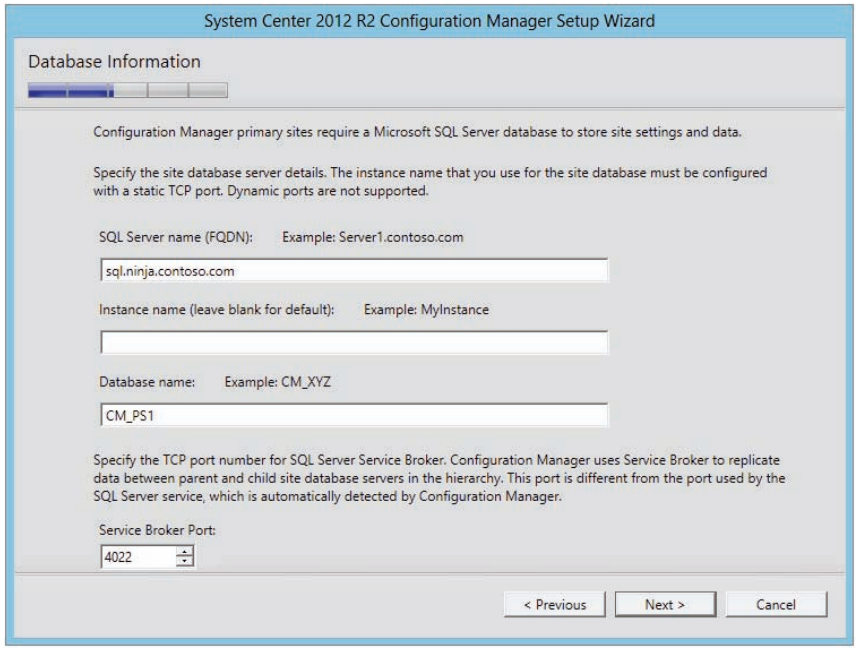


FIGURE 4.11
Setup Wizard: Database Information page for a primary site

If you had selected the Use Typical Installation Options For A Single Server Installation option on the Getting Started page, this screen of the wizard would have been suppressed.

7. Configure the settings on Database Server page as before.

8. Continue through the wizard as before until you arrive at the Client Computer Communication Settings page, shown in Figure 4.12.

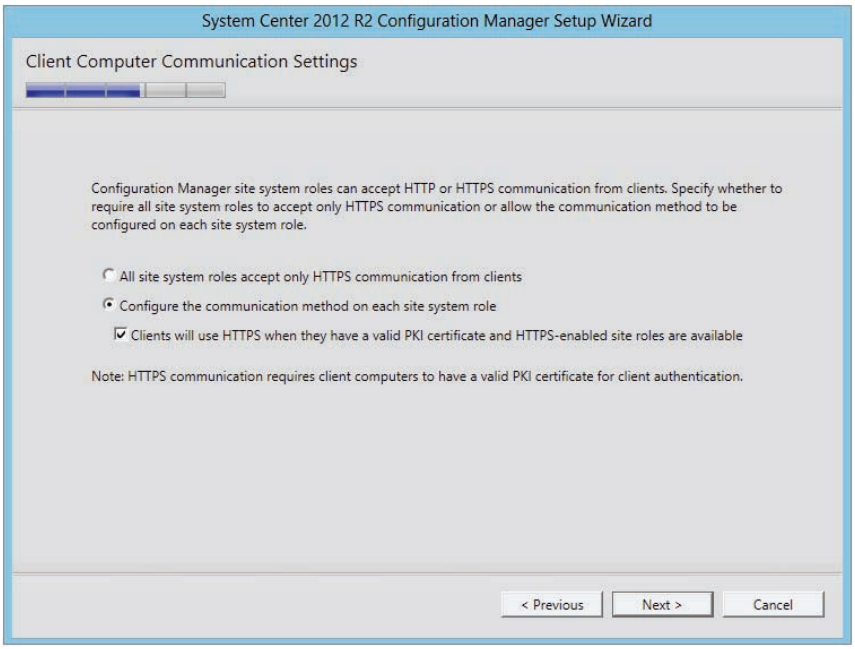


FIGURE 4.12
Setup Wizard: Client Computer Communication Settings page for a primary site

9. On the Client Computer Communication Settings page, decide whether clients will require secure HTTP communications or whether they can use either secure or non-secure HTTP communication.

   For the example, choose the latter option, and ensure that the box for Clients Will Use HTTPS When They Have A Valid PKI Certificate And HTTPS-Enabled Site Roles Are Available is selected. Setting this option ensures that when secure communications are possible, they are used.

10. Click Next to proceed to the Site System Roles page, shown in Figure 4.13.

11. On the Site System Roles page, configure whether or not setup should attempt to install a management point and/or a distribution point and, if so, on what server they should be installed and what communication protocol they should be using—either HTTP or HTTPS.

    Remember, site system roles do not have to be configured on the site server itself. Often the management point role is configured on the site server and the distribution point role is configured on both the site server and remote servers. For our example the management point and distribution point will be configured on the site server to use HTTP communication.

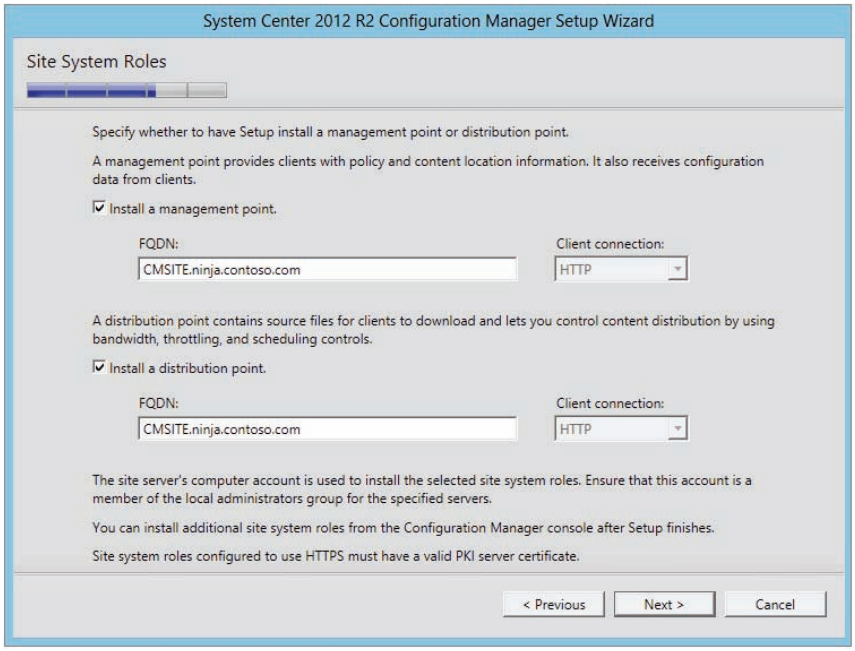


FIGURE 4.13 Setup Wizard: Site System Roles page for a primary site

FURTHER INDICATION OF CENTRAL ADMINISTRATION SITE UNIQUENESS

Notice that the option to specify a management point and a distribution point was not a part of the Central Administration Site Setup Wizard. This is another aspect of the fact that the Central Administration Site is different from a standard primary site. As already mentioned, the Central Administration Site cannot host clients, and therefore there is no need for a management point or distribution point.

12. Once this is configured, click Next, and complete the wizard as previously described and allow the primary site server to complete installation. Be sure to fix any relevant prerequisite failures!

If all goes well, the site should be installed. It's time to move to our next type of site: the secondary site.

Implementing a Secondary Site

Secondary sites historically have been used to allow local access to distribution points across slower WAN links. The secondary site installation allowed communication of content from its primary parent site to be compressed and the sender to throttle communication across sensitive or slow WAN links. Such a configuration was the most compelling reason for a secondary site installation in the past.

There are other reasons to maintain secondary sites in a hierarchy. One such reason would be if WAN links are too fragile to tolerate client traffic as policy data is retrieved from the management point and discovery and inventory data is uploaded to the management point. An example of such a condition would be a facility, such as a cruise ship, relying on unstable satellite connections for communications. In such a case a secondary site may still be needed.

The procedure for installing a secondary site in previous versions has been to either push the secondary site installation across the network or install the secondary site from installation media. You may have noticed that the Setup Wizard has no option to allow for installing a secondary site from media, which leaves only the first option—remote install of the secondary site—available in Configuration Manager 2012 R2. A remote install does *not* mean that media will need to be pushed to the target server. If media is available locally, then it can be used, or if not available locally, the needed content can be pushed. For our example, a secondary site will be installed as a child of the primary site just completed.

Initiate the secondary site from the Configuration Manager 2012 R2 administrative console. The installation can be initiated from either the Central Administration Server or the primary server. For the example, and since central administration is most commonly used, you'll start the installation from the Central Administration Site.

1. If the administrative console is not open on the Central Administration Site, open it by selecting Start ➢ All Programs ➢ Microsoft System Center 2012 R2 ➢ Configuration Manager ➢ Configuration Manager Console.
2. Once it is open, select the Administration workspace, and then expand Site Configuration ➢ Sites.
3. Select the primary site you just installed, and from the Home tab of the ribbon, choose Create Secondary Site, as shown in Figure 4.14. This action launches the Create Secondary Site Wizard.

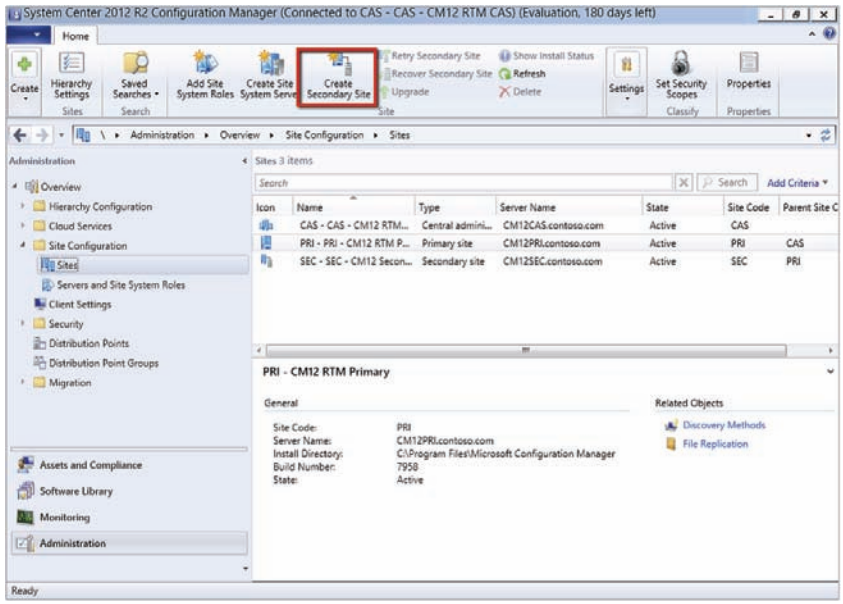


FIGURE 4.14 Secondary site installation

Note in the wizard that a management point and a distribution point will be installed on the secondary site. This is an important distinction because with previous versions administrators had a choice of whether to install a management point, known as a proxy management point, at a secondary site, or not. In Configuration Manager 2012 R2 there is no choice. As already mentioned, if you choose a secondary site configuration, it is assumed the WAN is too fragile to tolerate any unthrottled traffic and that local access to policy is required.

4. Review the remaining information on this page, and click Next to proceed to the General page, shown in Figure 4.15.

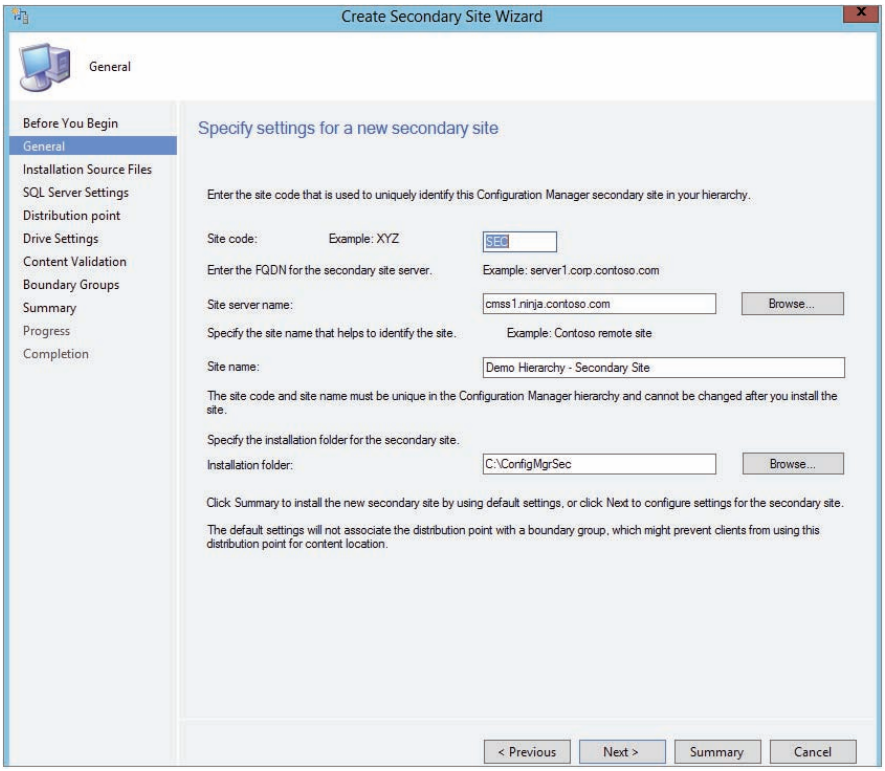


FIGURE 4.15 Create Secondary Site Wizard: General page

5. On the General page, provide information for the site code and the site name as well as the name of the site server where the secondary site will be installed and a path for the installation.

6. Click Next to proceed to the Installation Source Files page. Select whether to transfer the source files over the network, to use source files at a given network location, or to use source files already staged on or near to the remote system being selected for the secondary site installation.

The latter option allows for scenarios where the network link is insufficient or too unstable to reliably transfer data. For our example, data will be transferred across the network.

7. With the Copy Installation Source Files Over The Network From The Parent Site Server option selected, click Next to proceed to the SQL Server Settings page, shown in Figure 4.16.

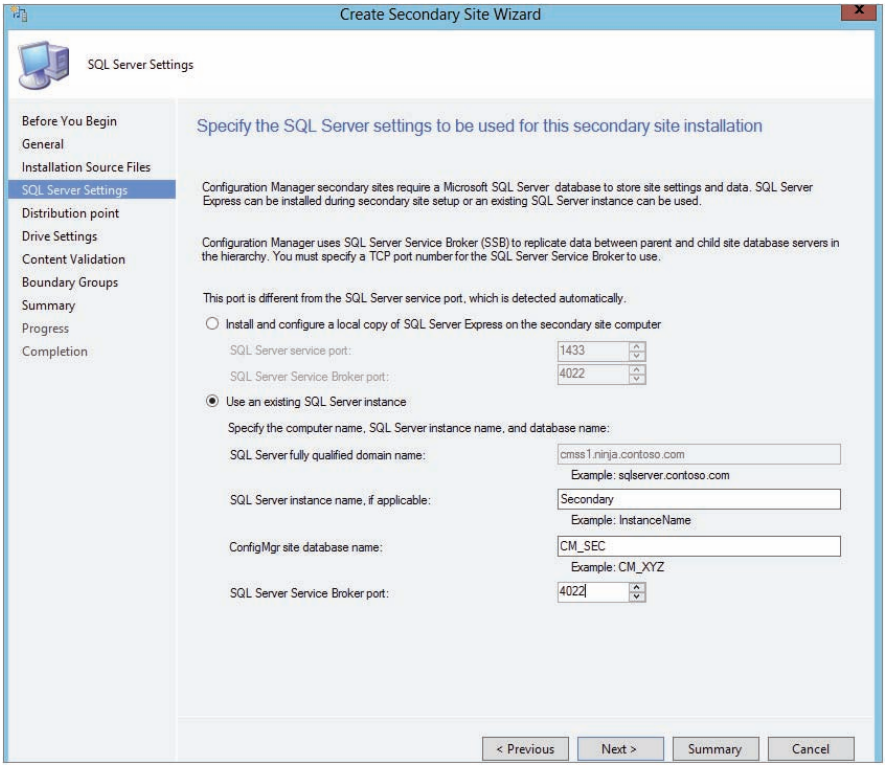


Figure 4.16
Create Secondary Site Wizard: SQL Server Settings page

8. On the SQL Server Settings page, either choose to install and configure SQL Express for the secondary server or, if an instance of SQL Server already exists on the destination server, choose the second option and enter details to configure the secondary site accordingly.

SQL and Secondary Site Servers

SQL may already be installed on the secondary site to support other applications, or it may be installed to support components needed by Configuration Manager, such as Windows Server Update Services. If it is, you may choose to install the secondary site database to the existing instance of SQL or choose to install SQL Express instead. If a full version of SQL is already installed, choosing to install SQL Express will result in another instance of SQL running.

Administrators with experience using previous versions of Configuration Manager may see the option to provide a database name and wonder whether they need to take manual action on the destination secondary site server to create the database. There's no need for concern. The installer will take the supplied database name and create the required database automatically.

For our example, SQL is already installed on the destination server, so follow these steps:

a. Select Use An Existing SQL Server Instance.

b. Supply SQL connection details.

c. Click Next to proceed to the Distribution Point page, shown in Figure 4.17.

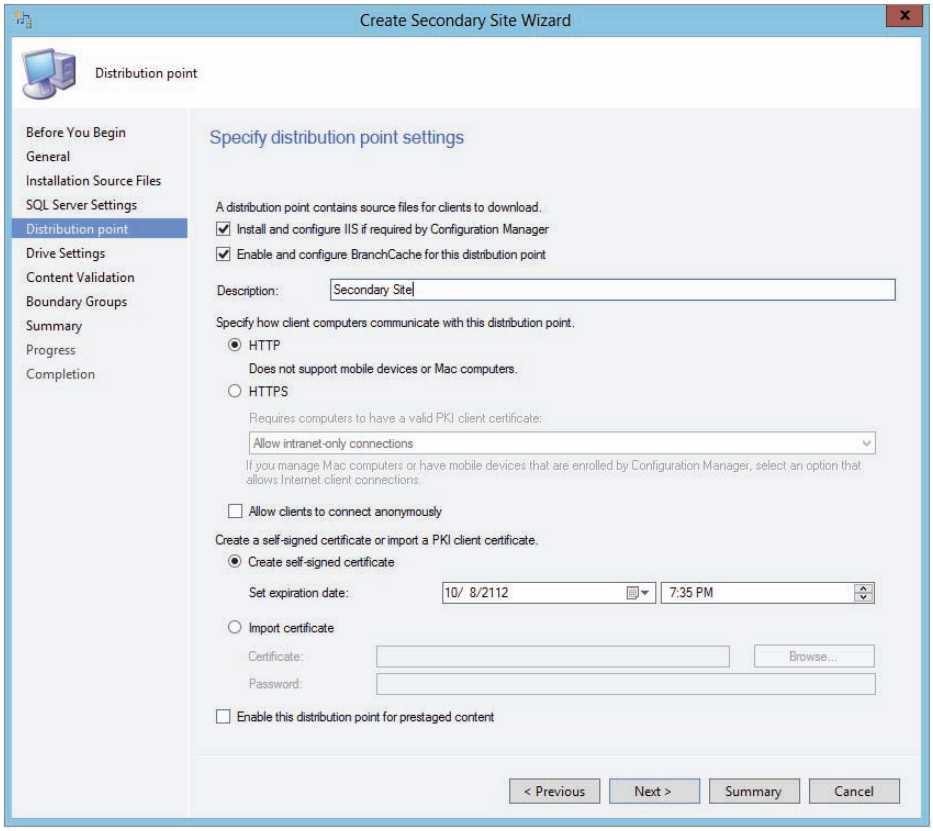


FIGURE 4.17 Create Secondary Site Wizard: Distribution Point page

9. On the Distribution Point page, choose the security options for how clients will communicate and also whether the distribution point will be enabled for prestaged content.

10. Click Next to proceed to the Drive Settings page, shown in Figure 4.18.

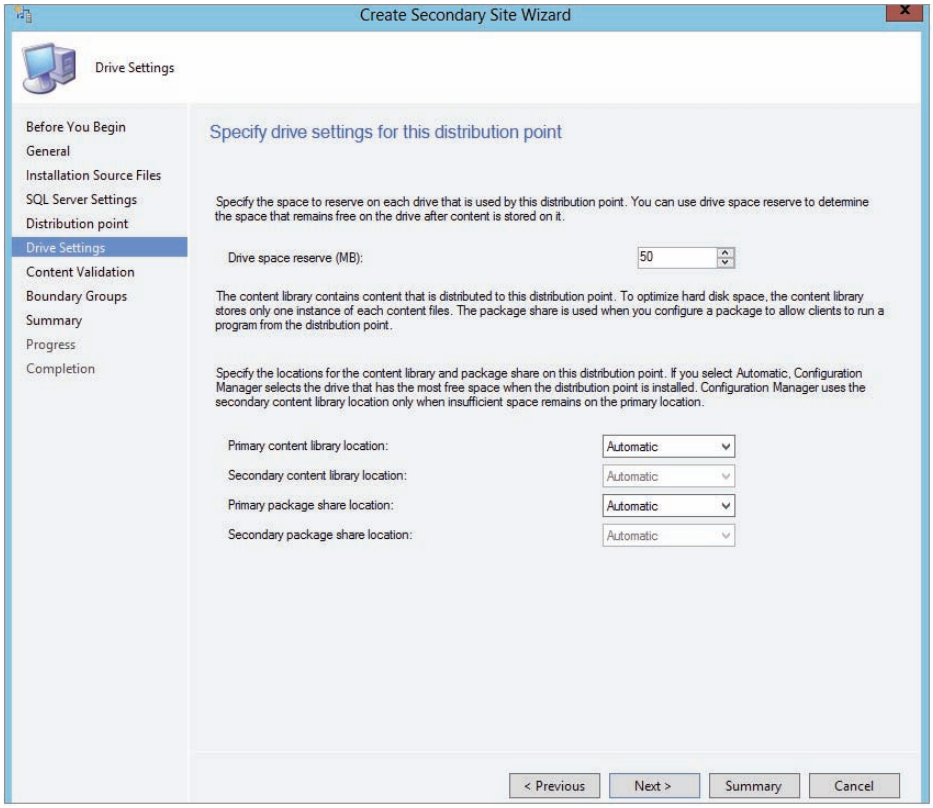


FIGURE 4.18
Create Secondary Site Wizard: Drive Settings page

On the Drive Settings page, configure how you would like your disk drives to be configured for use by the distribution point.

Click Next to proceed to the Content Validation page, shown in Figure 4.19.

On the Content Validation page, configure whether validation should take place and on what schedule and with what priority. Content validation is discussed in more detail in the Distribution Point site system role section later in this chapter.

11. Click Next to proceed to the Boundary Groups page. This page provides an opportunity to choose which boundary group the secondary site distribution point should join. There is no requirement to join a boundary group at this stage, and since none have yet been created during the install and further discussion of boundary groups is beyond our focus at the moment, we'll bypass configuring any options on this page.
12. Click Next to proceed to the Summary page, shown in Figure 4.20. This page displays the choices made in the Create Secondary Site Wizard.
13. Review the summary, and click Previous if you need to make any corrections. When finished, click Next to begin the secondary site installation.

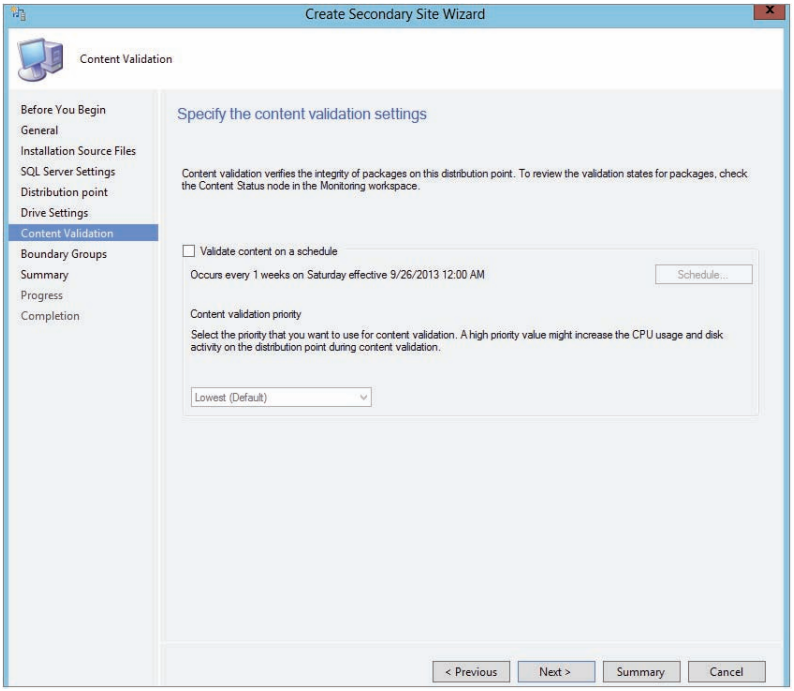


FIGURE 4.19
Create Secondary Site Wizard: Content Validation page

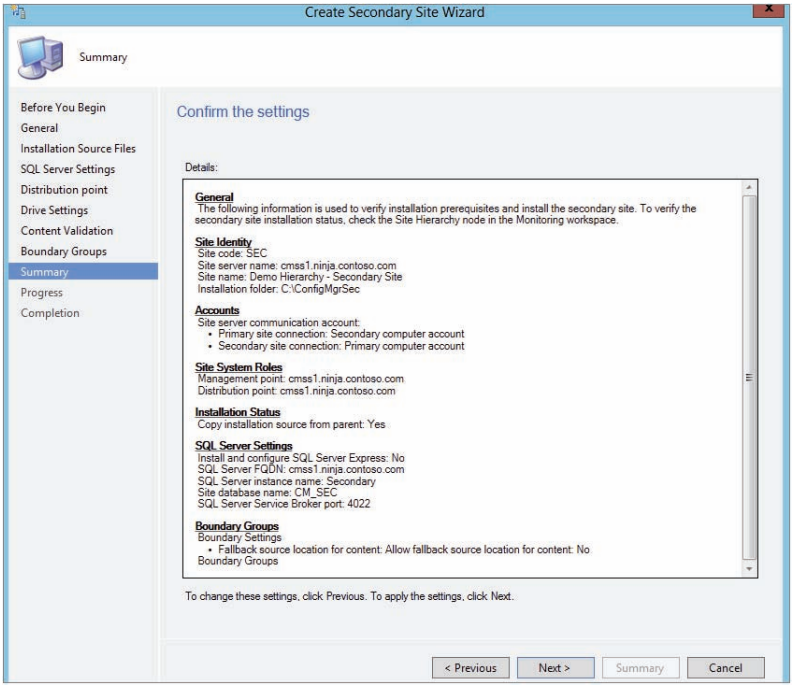


FIGURE 4.20
Create Secondary Site Wizard: Summary page

A progress page will come up while the secondary site installation job is being submitted, followed by the Completion page, which shows the installation details in roughly the same way as they appeared on the Summary page.

Installing a secondary site requires checking for prerequisites. This is done behind the scenes as a part of the installation. It is possible to review the prerequisite checks during secondary site installation in the console. Simply right-click the pending secondary site and select Show Install Status. The Secondary Site Installation Status screen is shown in Figure 4.21.

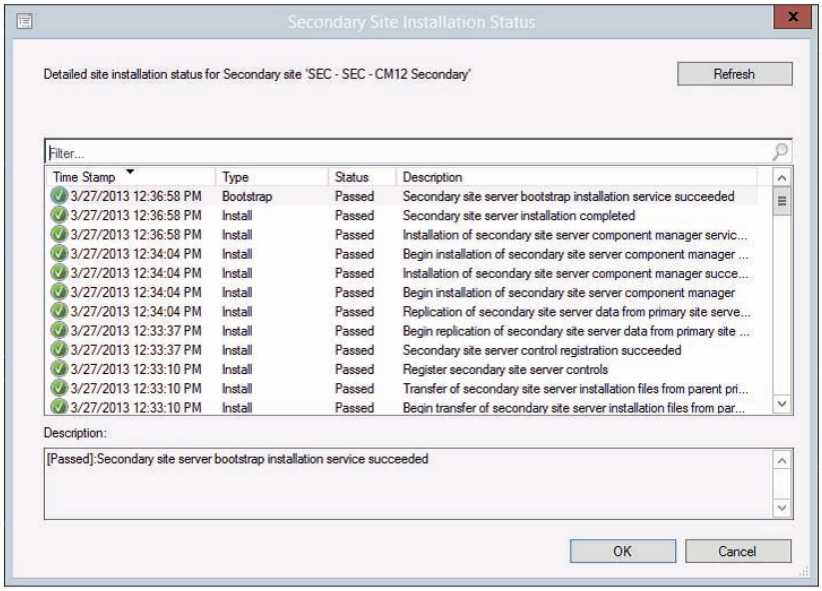


FIGURE 4.21 Right-click the secondary site and choose Show Install Status to see this screen.

Finally, a hierarchy is born! All that's left is to double-check the installations.

Verifying Proper Site Installation

It seems that all sites in our example installed successfully. The Administration console for the Central Administration Site shows all sites listed as expected and in an active state, as shown in Figure 4.22.

Based on this view alone, everything appears healthy. To make sure that this is truly the case, it's worth taking a look at a few key locations to verify. The locations to check may differ depending on the type of site being installed and the associated services chosen. We'll use the primary site as an example, but the topics generally apply to all types of sites. The areas discussed next are being presented to help with site installation validation. Providing the information in no way infers that it is OK to modify the described settings. In many cases Microsoft doesn't support modifying the settings, and doing so can result in a damaged site.

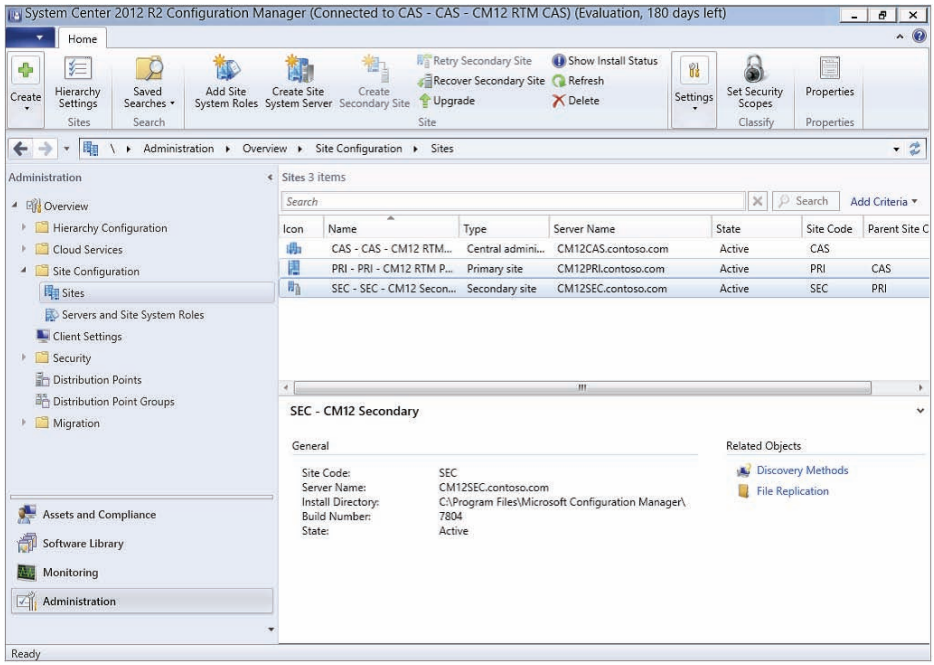


FIGURE 4.22 Administration console showing the Sites node

REGISTRY VALIDATION

A couple of registry locations are important for validating proper site installation. The locations that we discuss are not exhaustive of all registry keys that are added as part of site installation but rather are intended for use in spot-checking installation success.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS
```

It may be obvious but the `SMS` registry key is created as a result of site installation and should appear similar to Figure 4.23. The `Identification` key is selected to show some of the details about the site.

The `CCM` registry key is a shared key and will be present when either the management point component of a site server is installed or when a Configuration Manager 2012 R2 client is present on the system. If both are present, then the registry key is shared. The `CCM` key in this case is present because the installed site is a primary site, and the management point was installed as part of installing the site. If the management point is remote, the key won't necessarily be present on the site server. Note also that the client elements are missing from the registry key since the client is not yet installed at the site. This is shown in Figure 4.24.

The Central Administration server will not have the `CCM` key unless a client is installed on the system. The Central Administration server cannot host any clients and therefore cannot have a management point installed.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM
```

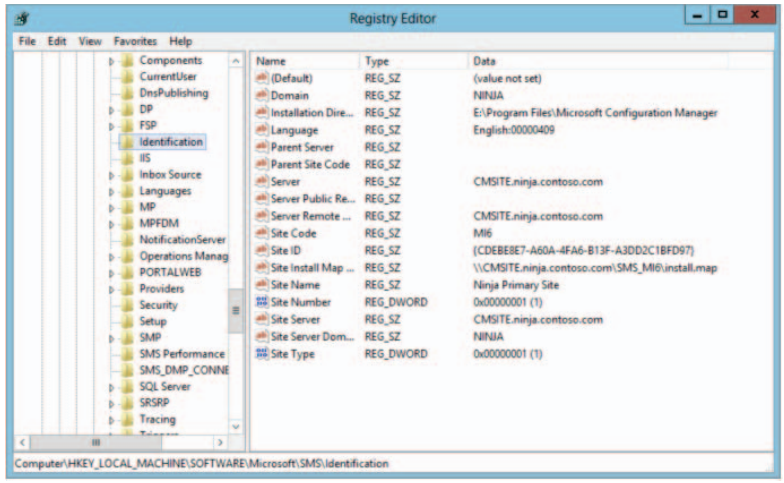


FIGURE 4.23
Post-installation `Identification` key

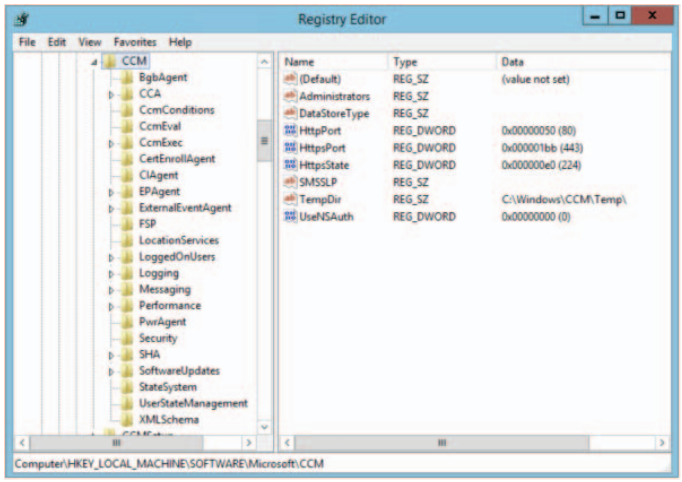


FIGURE 4.24
Post-installation `CCM` key

The `ConfigMgr10` registry key results from the console installation. Installing the console as part of the installation is optional, so this key may not be present. The key is shown in Figure 4.25.

```
HKEY_CURRENT_USER\Software\Microsoft\ConfigMgr10
```

The `Services` registry key is host to an abundance of keys for the various services running on the system. There will be a number of keys beginning with `SMS_` after a successful install. The number and type will depend on the type of site in question. This key is shown in Figure 4.26.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

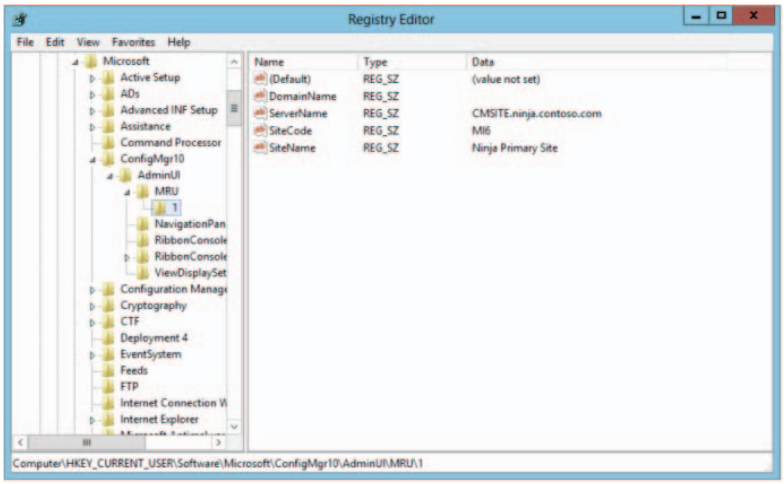


Figure 4.25
Post-installation `ConfigMgr10` key

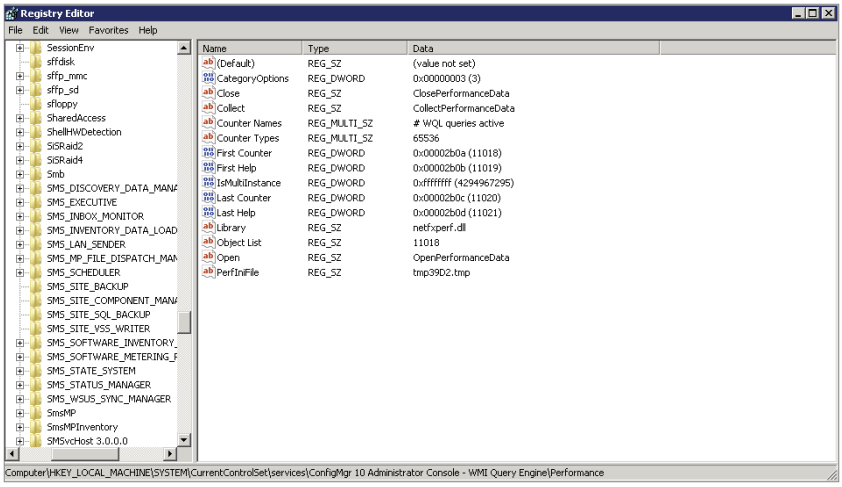


Figure 4.26
Post-installation `Services` key

File System Validation

Site installation files are located in a couple of different file locations. Pick the disk where Configuration Manager 2012 R2 was installed and navigate to ..\`Program Files\Microsoft Configuration Manager`. The folder will look similar to Figure 4.27. In addition, for sites with management points navigate to `Program Files\SMS_CCM`. The folder will look similar to Figure 4.28.

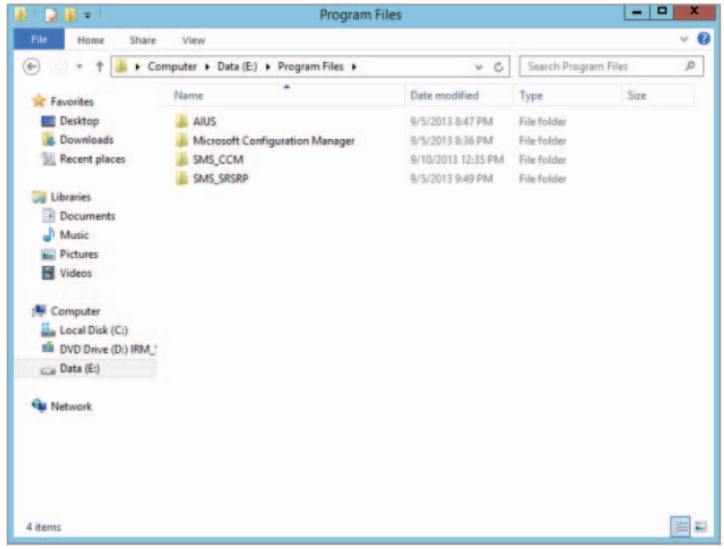


Figure 4.27
Microsoft Configuration Manager installation folder

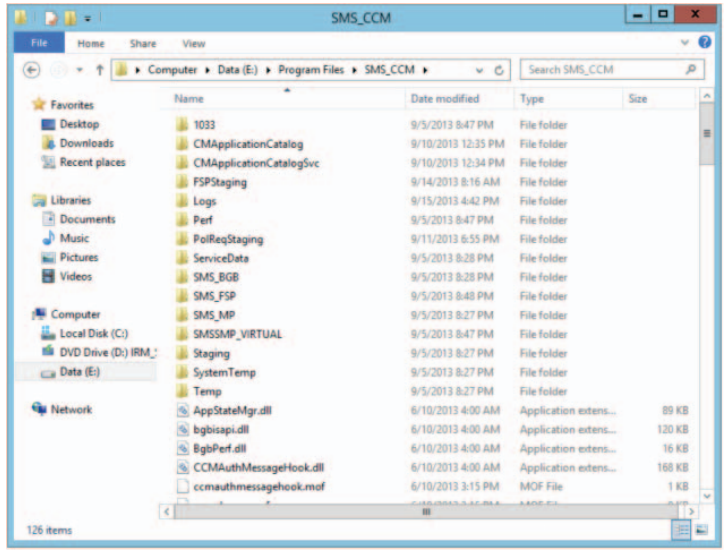


Figure 4.28
Management point SMS_CCM installation folder

Group Validation

The idea of a site hierarchy has been mentioned several times. In order to have a site hierarchy, the individual sites must be able to communicate. Detailed discussion about how this is done is beyond the scope of this chapter except to mention one thing: Communication between sites requires a security context. In Configuration Manager 2012 R2 such configuration is facilitated using groups configured on the site servers during installation. Several groups are created

during site installation, but only a single group, the SMS_SitetoSiteConnection_<site code> group, is used to configure the security context for site-to-site communication. When sites attempt communication, the default option is to do so with computer accounts. In the example hierarchy this would mean that when the Central Administration Site attempts to communicate with the primary site, it will attempt a connection using the computer account of the Central Administration account. This communication will fail unless the Central Administration Site's computer account is part of the SMS_SiteToSiteConnection_MI6 group. Said another way, any site that needs to communicate with the primary site must have its computer account as a part of the SMS_SiteToSiteConnection_MI6 group. This group is shown in Figure 4.29.

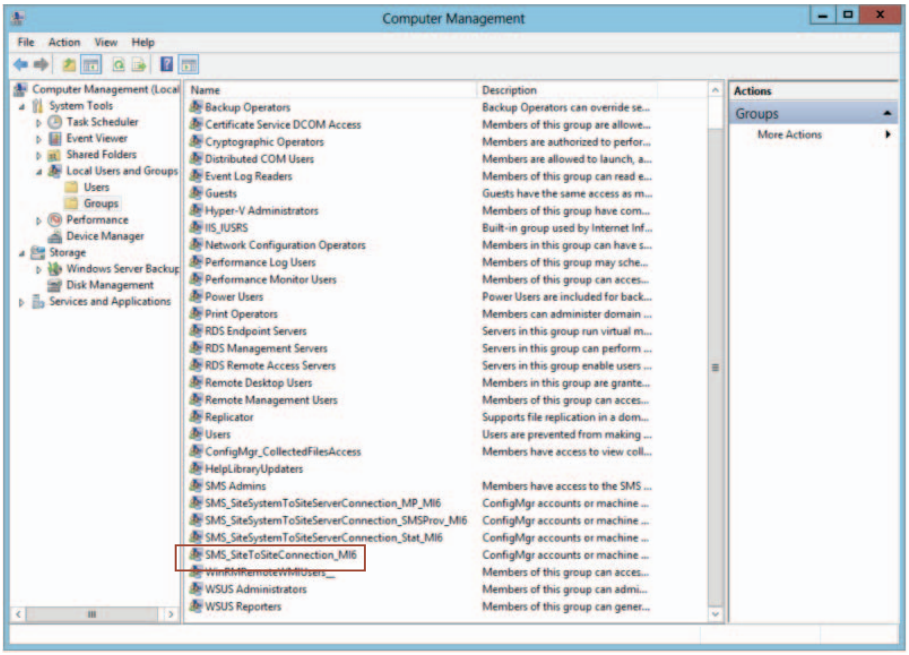


FIGURE 4.29
SMS_ groups added as part of installation

Adding Computer Accounts as Administrators

OK, it's not really true to say that the computer accounts must be members of the SMS_SiteToSiteConnection_<site code> group. Simply adding the computer accounts as administrators of the various servers would achieve the same purpose and is not recommended. Taking this approach grants more rights than are necessary to the computer accounts and is not a recommended method.

If you prefer not to use the computer accounts as administrators, then it is possible to configure specific credentials to facilitate site-to-site communication. Simply substitute those credentials for the computer account in the same group.

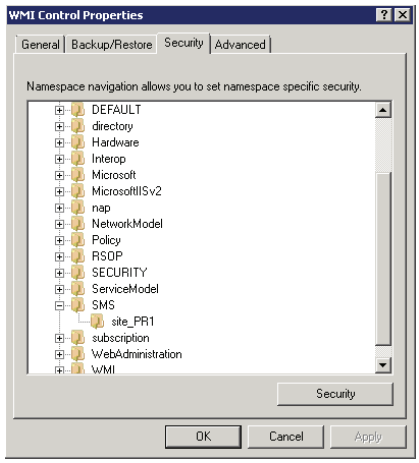
Windows Management Instrumentation Validation

We've already mentioned the idea of the SMS Provider. The SMS Provider is used to interact with the site server database, so ensuring that the installation created information in Windows Management Instrumentation (WMI) as required is important. The current discussion is not intended to be a detailed WMI discussion; simply ensuring that the namespaces were created as required is enough. To verify, follow these steps:

1. Open Computer Management.
2. Select Configuration and then WMI Control.
3. Right-click WMI Control and select Properties.
4. Select the Security tab and expand Root.

A successful installation will result in the SMS namespace being created along with the child namespace `site_<site code>`, as shown in Figure 4.30.

Figure 4.30
WMI namespace validation



Services Validation

The services have already been validated in the registry, but it's also a good idea to take a look at them in the Services list to ensure all are present and in the proper state of operation. This is shown in Figure 4.31.

Database Validation

A site can't work without its database, so it stands to reason that the site couldn't be installed successfully without the database being installed successfully. Very true, but it's still worth a look for familiarity if nothing else. To view the database, launch SQL Management Studio and follow the steps listed. In our example, SQL is located on the same server as the site.

1. Connect to the database.
2. Open the server.
3. Expand Databases, and the CM_MI6 example database should be present. This is shown in Figure 4.32.

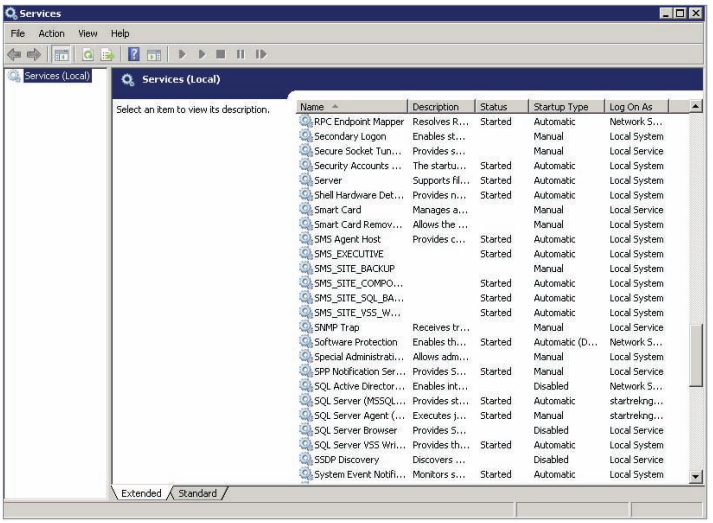


FIGURE 4.31
Services validation

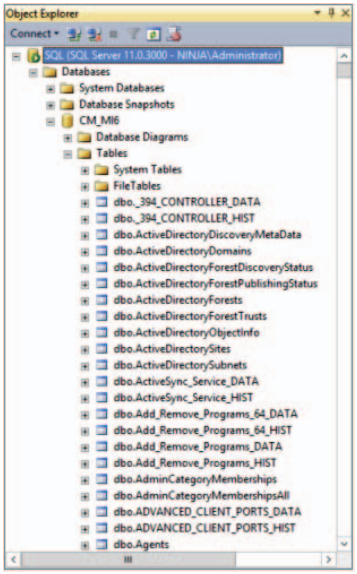


FIGURE 4.32
Database validation

Troubleshooting a Configuration Manager 2012 R2 Site Installation

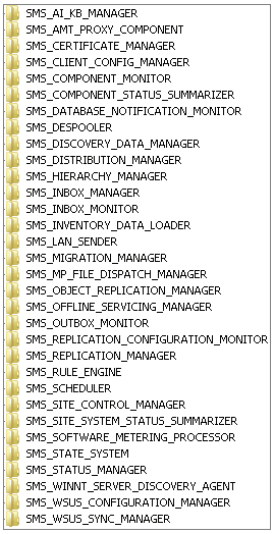
We've validated the hierarchy installation, but that doesn't guarantee the site is working properly. Configuration Manager has many moving parts, and at times problems will surface. Understanding how to troubleshoot those problems is important to maintaining a healthy Configuration Manager hierarchy. So where should you look to troubleshoot issues with a site? Let me first say that this chapter is not an exhaustive troubleshooting chapter. Troubleshooting is covered in some depth in Chapter 19, "Troubleshooting." Still, it's helpful to know how things have

progressed for a site installation. Fortunately, Configuration Manager is not lacking in information to help administrators check for problems and ascertain the nature of the problems. As with validation, this brief troubleshooting discussion will focus on the primary site that was installed.

The key component in place at a site, whether that site is the Central Administration Site, a primary site, or a secondary site, is the `SMS_Executive` component. This one service orchestrates most every activity at a site, and the list of `SMS_Executive` threads is extensive. Figure 4.33 is a screenshot of the various threads that run as part of the `SMS_Executive` component.

Since this is such a key service for all sites, it's a good idea to check the status of the Executive service in general to make sure all is well. Details on the various threads of the `SMS_Executive` component will mostly be left for later.

FIGURE 4.33
`SMS_Executive` threads



There are several ways to view details on the status of `SMS_Executive`. First, Configuration Manager provides a robust status message system so administrators can tell at a glance if all is good with a particular component. Take a look at the Monitoring ➢ System Status ➢ Component Status node of the administrative console; the `SMS_Executive` component, along with all of the other threads, is visible. A quick look shows that the status of this thread is OK, as shown in Figure 4.34. Note that the `SMS_Executive` component from all three sites is displayed here.

Status messages are not shown in real time, and there may be some short lag in reporting an error condition or reverting to an OK condition if a component is again running healthy.

If the status is not OK or you need more details about this component, you can see them by right-clicking, selecting Show Messages, and selecting what kind of messages are of interest. On the context menu is also the Reset Counts option, which will reset to 0 any error counts being held for the various types of messages, errors, and warnings. You can take this action after resolving an issue and to restart tracking of a component.

Another way to view the status of a component, and the method preferred by many administrators, is to take advantage of the extensive logging system provided in Configuration Manager. The logs are located in the Microsoft Configuration Manager ➢ Logs directory on the

site server. Just as the status system showed the various components, there are logs representing them as well. The names aren't identical to the component names, but they are very similar and generally easy to correlate. In the case of the `SMS_Executive` component, the corresponding log is `smsexec.log`, as shown in Figure 4.35.

These log files can be viewed directly in Notepad, but the native CMTrace log viewer utility is preferred because it formats the logs nicely and also allows monitoring logs in real time as they are written.

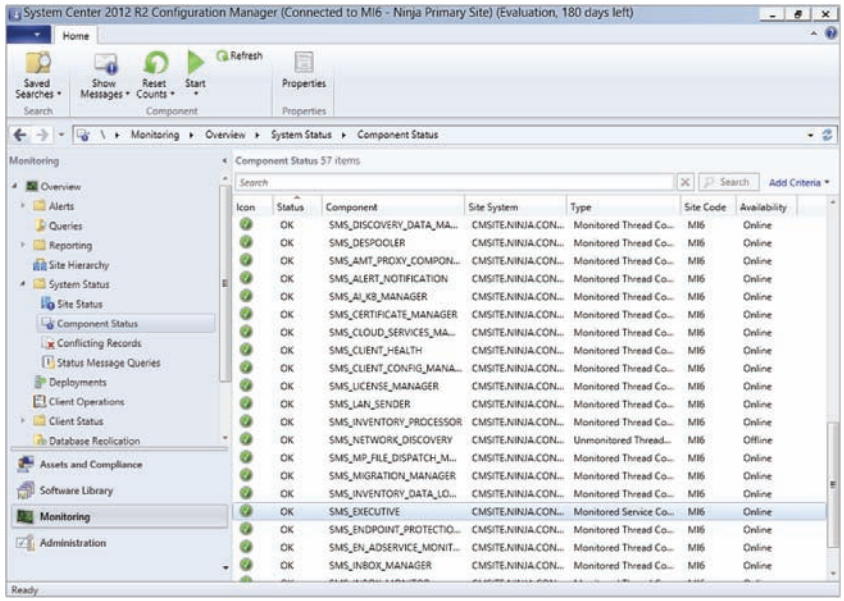


FIGURE 4.34 `SMS_Executive` component status

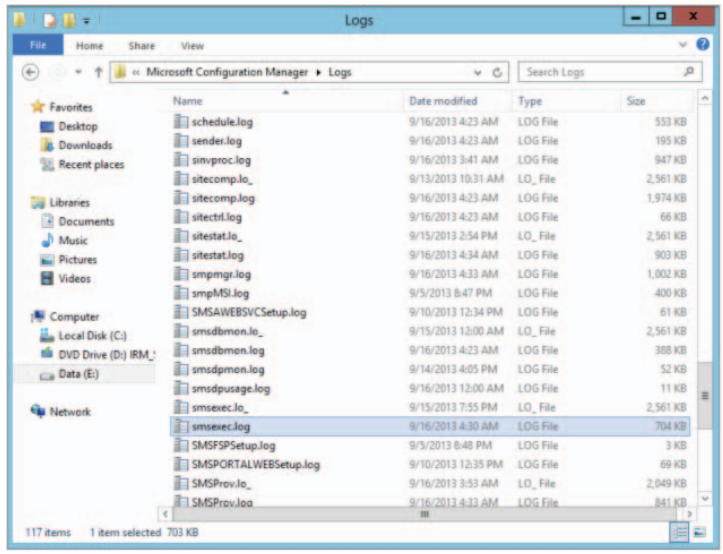


FIGURE 4.35 `smsexec.log` file

Good Old Trace32

Configuration Manager 2012 introduces an updated version of Trace32. The new name is CMTrace. Previous versions of the Trace32 utility may have problems if used in Configuration Manager 2012 R2. The updated utility is available in the `Tools` folder on the Configuration Manager 2012 R2 media.

Like Trace32, the CMTrace utility is very flexible, and administrators will find it to be useful for examining logs other than those from Configuration Manager.

Another critical component of the site is the site server database. Without the database, the site fails to function. To that end, you must understand how to at least begin an investigation of the database should problems arise. The database status can be seen in the Monitoring node of the Configuration Manager console as well. In terms of the database, isolating specific components to troubleshoot is difficult because it really does depend on the problem at hand. However, two components are fairly important for interaction with the database: the SMS Database Monitor and the SMS Provider.

SMS Database Monitor The SMS Database Monitor, represented in the Monitoring node as `SMS_Database_Notification_Monitor` and in the logs as `smsdbmon.log`, is responsible for monitoring actions that are taken by the administrator in the console and for taking steps to implement those changes by notifying the various components of the `SMS_Executive` component that work is waiting to be done.

SMS Provider The SMS Provider is important because it is the conduit between most console actions and making those actions effective in the database. As an example, when an administrator selects a site to view in the console or makes changes to a console setting, the SMS Provider interacts with the SMS database via WMI to retrieve needed data or make changes to data. Without the SMS Provider the site cannot function.

Another useful location for quickly checking the status of the database and more is again in the Monitoring node but this time under Site Status. In this node it's quick to see the amount of disk space available for various components that make up a site. This node is shown in Figure 4.36.

Unattended Installation

In some cases it may be of interest to perform a scripted install of Configuration Manager. This chapter won't go into depth about how this process works, but suffice it to say that the most difficult part of installing a site often is the *answer file* used during installation. Configuration Manager 2012 R2 makes this easier by the fact that when a site is installed through the UI, an unattended installation file is created as part of the process. This unattended file is called `ConfigMgrAutoSave.ini` and is located in the `temp` directory for the user installing the product. The file is easily modified to perform scripted installs of other sites.

The unattended files generated in the example are shown to give an idea of how these are constructed based on different site types. When you're using the unattended file to initiate a site installation, a command line similar to the following should be used:

```
Setupwpf.exe /script <path to script>\ConfigMgrAutoSave.ini
```

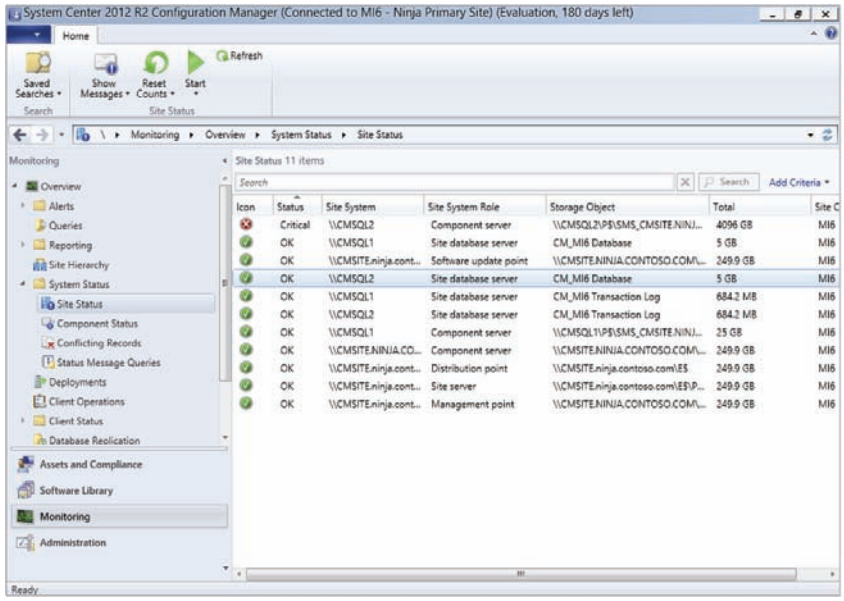


FIGURE 4.36
Site Status Monitoring node

This command line should be initiated from within this directory:

```
<Configuration Manager Source>\SMSSetup\BIN\x64
```

The content of the unattended files is shown in Listing 4.1 and Listing 4.2. Note, single lines may wrap for readability.

LISTING 4.1: Central administration site unattended file

```
[Identification]
Action=InstallCAS

[Options]
ProductID=
SiteCode=CAS
SiteName=Demo Hierarchy - Central Administration Site
SMSInstallDir=C:\Program Files\Microsoft Configuration Manager
SDKServer=cmcas.contoso.com
PrerequisiteComp=0
PrerequisitePath=C:\SCCM2012Updates
MobileDeviceLanguage=0
AdminConsole=1
JoinCEIP=0

[SQLConfigOptions]
SQLServerName=cmcas.contoso.COM
DatabaseName=CM_CAS
```

```
SQLSSBPort=4022
SQLDataFilePath=C:\Program Files\Microsoft SQL Server\MSSQL10_50
.MSSQLSERVER\➥
MSSQL\DATA
SQLLogFilePath=C:\Program Files\Microsoft SQL Server\MSSQL10_50
.MSSQLSERVER\➥
MSSQL\DATA

[HierarchyExpansionOption]
```

Listing 4.2: Primary site unattended file

```
[Identification]
Action=InstallPrimarySite

[Options]
ProductID=
SiteCode=PS1
SiteName=Test Hierarchy - PS1
SMSInstallDir=C:\Program Files\Microsoft Configuration Manager
SDKServer=cmps1.contoso.com
RoleCommunicationProtocol=HTTPorHTTPS
ClientsUsePKICertificate=1
PrerequisiteComp=1
PrerequisitePath=\\cmcas\c$\sccm2012updates
MobileDeviceLanguage=0
ManagementPoint=cmps1.contoso.com
ManagementPointProtocol=HTTP
DistributionPoint=cmps1.contoso.com
DistributionPointProtocol=HTTP
DistributionPointInstallIIS=0
AdminConsole=1
JoinCEIP=0

[SQLConfigOptions]
SQLServerName=cmps1.contoso.com
DatabaseName=CM_PS1
SQLSSBPort=4022
SQLDataFilePath=C:\Program Files\Microsoft SQL Server\MSSQL10_50
.MSSQLSERVER\➥
MSSQL\DATA
SQLLogFilePath=C:\Program Files\Microsoft SQL Server\MSSQL10_50
.MSSQLSERVER\➥
MSSQL\DATA

[HeirarchyExpansionOption]
CCARSiteServer=cmcas.contoso.com
```

Installing Site System Roles

The process just discussed results in a hierarchy with three sites: a Central Administration Site, a primary site, and a secondary site. But just installing the sites doesn't mean that installation is complete. In order to provide service to clients that will be *interacting* with these sites, you must first decide what services will be provided and then configure the additional site components that facilitate providing the needed services. These site components are also known as *site system roles*. The ones available for a given site will depend on the site type:

Central Administration Site

- Asset Intelligence synchronization point
- Certificate registration point
- Endpoint protection point
- Reporting Services point
- Software update point
- System Health Validator point
- Windows Intune Connector

Primary site

- Application Catalog web service point
- Application Catalog website point
- Certificate registration point
- Enrollment point
- Enrollment proxy point
- Fallback status point
- Out of band service point
- Reporting Services point
- State migration point
- System Health Validator point

Secondary site

- Software update point
- State migration point

Notice that the term *interacting* was used in regard to clients and site servers. Administrators familiar with Configuration Manager may have expected the term *assigned* to be used instead. This term was used on purpose because in Configuration Manager clients can only be assigned to primary sites but are able to interact with any site their boundaries match. This concept is

known as *roaming* and describes how clients are able to interact with secondary sites and other primary sites if they're within defined boundaries for those sites. Roaming is beyond the scope of discussion for this section.

A common element in installing all site system roles is the Add Site System Roles Wizard. Before launching the wizard to add the role, you must first decide whether the role will be added to an existing server or a new server. In the example hierarchy just built, that means a choice of adding the new role to a site server itself or creating a new server on which to add the role (both are shown in Figure 4.37).

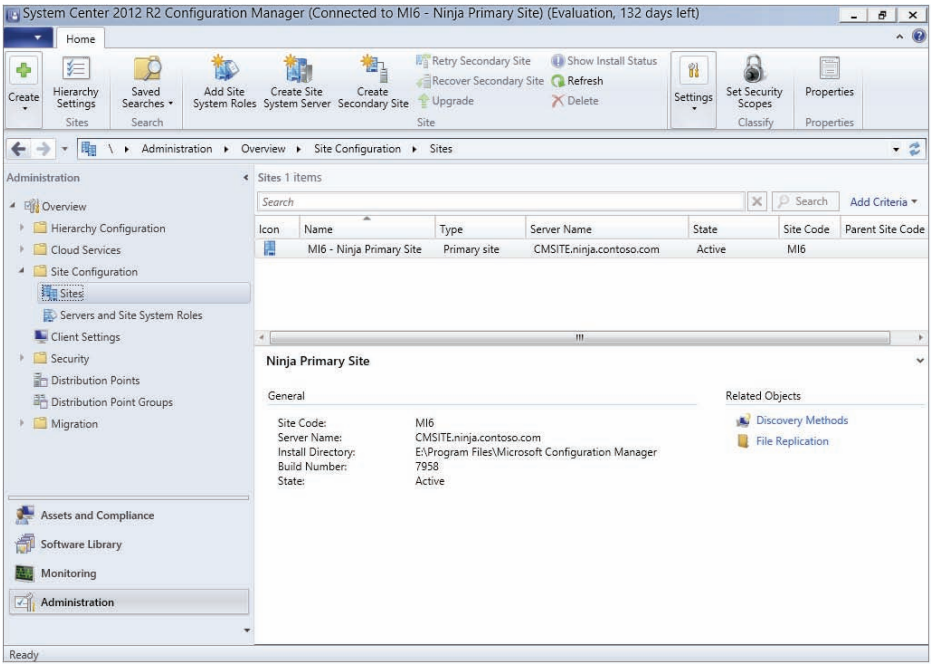


FIGURE 4.37
Use the Create Site System Server button on the ribbon to create a new server; use the context menu to assign a new role on an existing server.

- If you're adding to an existing server, simply right-click that server under the Servers and Site System Roles node of the console, and choose Add Site System Roles.
- If you're adding a new server to host a site system role, that process is initiated by selecting the Create Site System Server action from the Home tab of the ribbon.

A single remote site system server cannot host roles from multiple sites!

Both methods will result in the Create Site System Server Wizard being launched. The only difference is whether the server name field will be populated and grayed out, and there is no option to specify the site code that the new server should support since it is already part of a site. For the example, site system roles are being added to the primary site, which already exists. The first page of the wizard is shown in Figure 4.38.

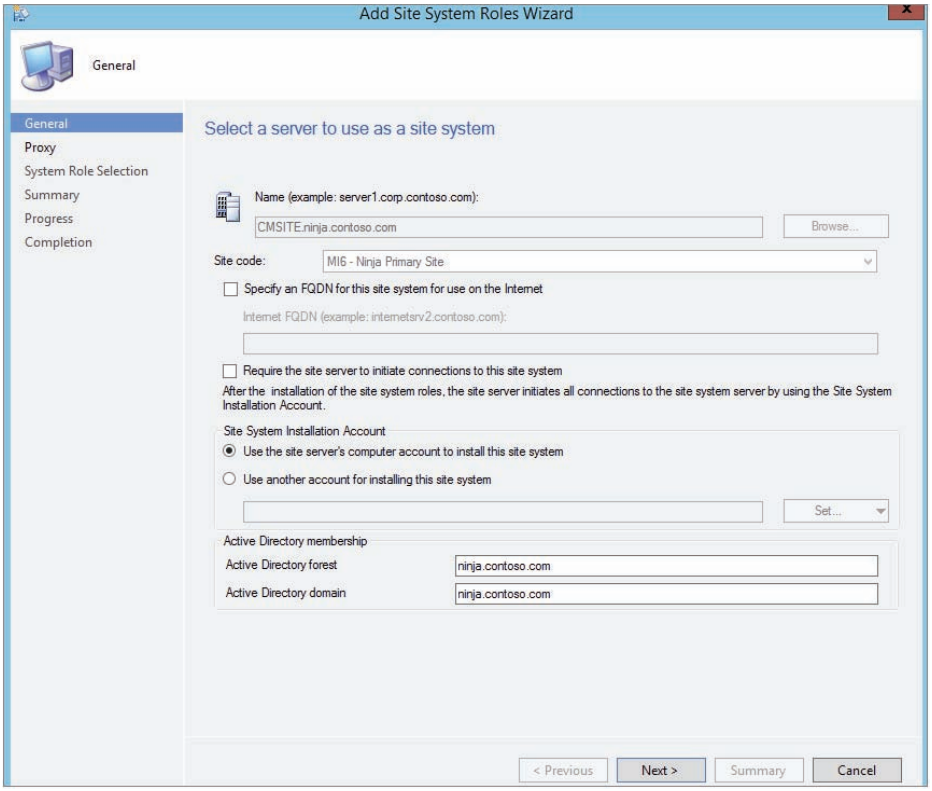


FIGURE 4.38
Add Site System Roles Wizard: General page

On this page of the wizard you have the opportunity to provide a server name. This option will be available only if you're creating a new site system server. In addition, options are available to supply the FQDN of the server if it will be addressable from the Web. This option was also available in Configuration Manager 2007, but this brings up an interesting point of discussion. Configuration Manager 2007 supported two security modes: standard security and native mode security. Native mode security was required when specific functions were to be used, such as Internet-based client management and mobile device management. Native mode as a security option in Configuration Manager 2012 is gone and has been replaced by the ability to designate site system servers as those that will participate on the Internet or serve other functions that require certificate-based security. In this way the additional security afforded by certificates can be applied just where it's needed—to the site system itself.

The option Require The Site Server To Initiate Connections To This Site System appears to be new but is actually just a relabeling of the Configuration Manager 2007 option that was on this page: Allow Only Site Server Initiated Data Transfers From This Site System. The goal of this option, as the wizard states in Configuration Manager 2012, is to designate that communication to site systems should be initiated from the site server itself rather than the site system pushing data back to the site server. This adds additional security and also accommodates scenarios where trusts aren't in place to accommodate cross-forest authentication.

Administrators accustomed to previous versions of Configuration Manager may note that the option to set the site system as a protected site system is no longer available on the first page of the Create Site System Server Wizard. Site system protection only ever applied to distribution points and state migration points. Based on the new design of Configuration Manager 2012 R2, meaning distribution points and state migration points are protected by default (more on that shortly), the option to do so was not needed on the Create Site System Server Wizard.

Clicking Next on the wizard will move you to the node to allow you to select which site system roles should be added to the target server. Once you select the roles and continue moving through the wizard, you must configure the various options for the role-specific pages that will be displayed. Those pages will be discussed shortly for each type of site system.

As previously stated, the available site system roles for a given server depend on the type of server being configured. Each available site system role is described next.

Understanding Configuration Manager 2012 R2 Site System Roles

The various site system roles available for each site type can be seen using the administrative console and focusing on the site in question. The list of available site systems that might be installed at the Central Administration Site, for example, can be obtained by doing this:

1. Open the console and navigate to Administration ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Select the site type of interest, right-click, and choose Add Site System Roles.
3. In the wizard, move to the System Role Selection page.
4. Compare the roles available on this page to the roles already installed for the site, as shown in the console.
5. Then, generate a full list of available roles for a given site.

You can use the same approach for obtaining lists of available site systems for a primary site and a secondary site. Table 4.1 shows the available sites for each site type.

TABLE 4.1: Available site system roles by site type

SITE SYSTEM ROLES	CENTRAL ADMINISTRATION SITE	PRIMARY SITE	SECONDARY SITE
Component server	×	×	×
Distribution point		×	×
Management point		×	×
Site database server	×	×	×

TABLE 4.1: Available site system roles by site type *(CONTINUED)*

SITE SYSTEM ROLES	CENTRAL ADMINISTRATION SITE	PRIMARY SITE	SECONDARY SITE
Site server	×	×	×
Site system	×	×	×
System Health Validator point	×	×	
State migration point		×	×
Fallback status point		×	
Out of band service point		×	
Reporting Services point	×	×	
Application Catalog web service point		×	
Application Catalog website point		×	
Mobile device enrollment proxy point		×	
Mobile device and AMT enrollment point		×	
Asset Intelligence synchronization point	×		
Endpoint Protection point	×		
Software update point	×	×	×
Windows Intune Connector	×	×	
Certificate registration point	×	×	

Notably missing from the list of roles at the Central Administration Site is the management point role and the distribution point role. This might seem strange at first until you again factor in that a Central Administration Site is not intended to support any clients; it is solely for the purpose of administration.

Also notably missing are the PXE service point role for operating system deployment and the Server Locator Point role used to help clients during site assignment and management point lookup. Don't worry, neither role is gone. The PXE service point is now available as a component of the distribution point role and the Server Locator Point has been merged into the management point role.

Another interesting aspect is that one of the site system roles listed for each site is the site server itself. That may seem odd, but in truth the site server function is but one role, albeit the key one, for a site. Note also that these roles can be placed on the same server or they can be placed on dedicated servers. The decision is driven by client count and load on a given role. For some site systems types such as distribution points (discussed shortly), it's quite possible that the same role will be needed on multiple servers to support a single site.

Now, let's discuss what each site system role does, the services it delivers, how it can be used, and some tips on troubleshooting each role.

Component Server

A *component server* is a unique site system role in Configuration Manager. This role cannot be manually added, nor can it be manually removed. This role is managed by the site server itself and will exist on any server that is running the `SMS_Executive` service within the hierarchy. This service runs specified threads that support other roles such as a management point.

Troubleshooting a Configuration Manager Component Server

This role manages the threads of the `SMS_Executive` service. It maintains which roles are local and remote for a given site. The overall health of the site server role can be reviewed in the Monitoring node. You can review the following logs to gain insight into the component server health:

`sitecomp.log` This log shows all the site roles and where they're configured to be running.

`compmon.log` This log records the status of all the threads of the `SMS_Executive` service and writes that status to the system registry under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Operations Management`. This information is used to keep track of component status and is also used as a resource for System Center Operations Manager in monitoring the status of Configuration Manager.

Distribution Point

The *distribution point* role has been expanded in Configuration Manager 2012 R2. In previous versions this site system was nothing more than a glorified file server, storing files for access by clients requiring content.

The role of the distribution point is still to store file content and make it available to clients, but the way in which it does this has been updated. The first thing that we should mention is that the distribution point is designed to support both classic package distribution and the new application distribution mechanism introduced in Configuration Manager 2012 R2. The legacy style distribution point, which is noted by a file folder named `SMSPKG<driveletter>$`, remains but is used only for packages set to Run from Distribution Point, and this is the only deployment mechanism that bypasses the requirement to use Background Intelligent Transfer Service (BITS). Beyond that, the updated distribution point structure is used universally. While the function of the distribution point in Configuration Manager 2012 R2 remains the same, making content available to clients, the structure and function of the distribution point to provide its service have been substantially updated.

- There is no option to use the distribution point without making use of BITS.
- The distribution point structure is no longer just a file store. Now, files are stored in a cache that takes advantage of single-instance storage, supports automated integrity checks, and more.
- The branch distribution points are gone and replaced with the fact that a standard distribution point is now fully supported on a supported Windows 7 workstation system, no client required. The workstation system is still subject to the connection limitation for a given operating system. In Windows XP administrators were accustomed to a connection limit of 10. In Windows 7 the connection limit increased to 20.

Bottom line, this isn't your grandpa's distribution point anymore! First things first—the distribution point must be installed.

It may be that the distribution point role is already installed. One of the default settings when installing a primary or secondary site is to also add the distribution point and management point roles. If the role has not yet been added or if an additional distribution point is needed, then this component won't yet be present on the server and will need to be added.

1. In the Create Site System Server Wizard, and as shown in Figure 4.39, select the distribution point role, and click Next to proceed to the Distribution Point page of the wizard, as shown in Figure 4.40.

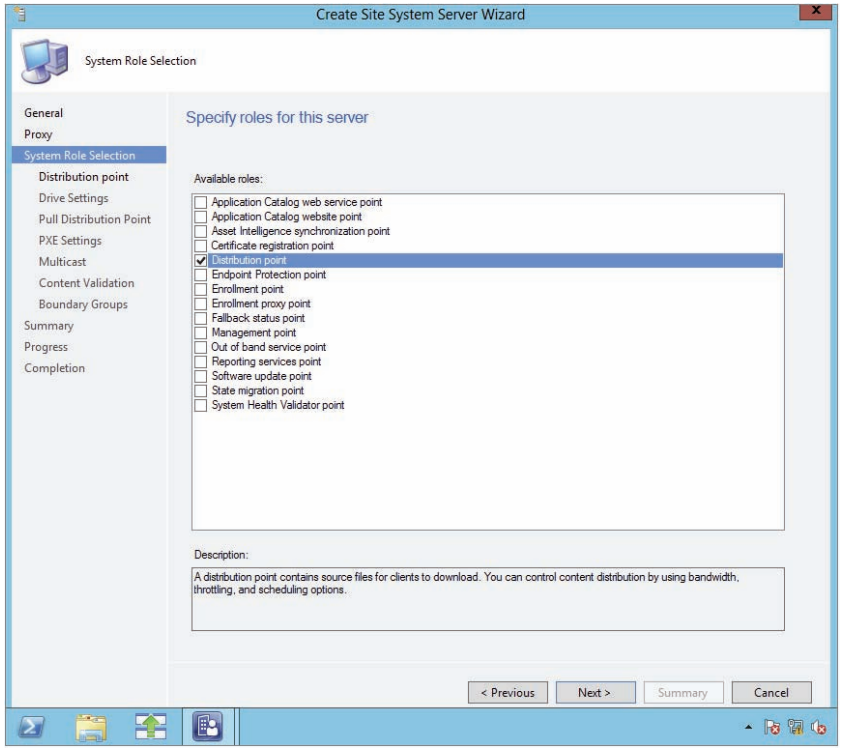


FIGURE 4.39 Create Site System Server Wizard: distribution point selected

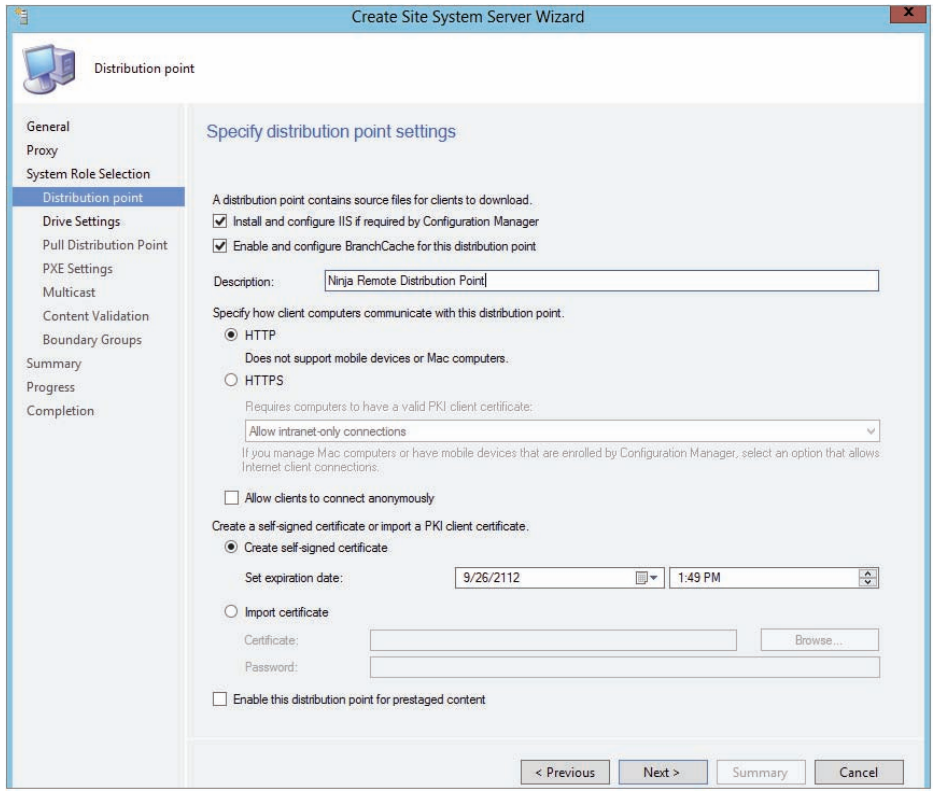


FIGURE 4.40 Create Site System Server Wizard: Distribution Point page

2. On the Distribution Point page of the wizard, configure a few options:
   - The first option, Install And Configure IIS If Required By Configuration Manager, is not selected by default, but you must select this option prior to proceeding. This option highlights the fact that with Configuration Manager 2012 R2 it is not possible to create a non-BITS-enabled distribution point. This fact may influence distribution point placement but is a welcome modification for sure. Also in this section you can select Enable And Configure BranchCache For This Distribution Point. BranchCache is a feature introduced with Windows Server 2008 R2 that allows systems within the same subnet and separate from a content source to share downloaded content locally rather than each system having to download them. You can also enter any information as a description of this distribution point; it's a good idea to configure this to verify what this distribution point is for.
   - Next on the page is the choice of whether clients should communicate with the distribution point using HTTP or HTTPS traffic. When clients use BITS to pull information from the distribution point, as is required by Configuration Manager 2012 R2, the clients do not directly connect to the distribution point structure but rather initiate a BITS session through IIS.

- Other options on this page allow the administrator to decide whether the distribution point will use self-signed certificates or certificates imported from a different source, such as a certificate authority. If the installation supports Internet scenarios, a certificate would be imported at this step.
- The last option on the page allows configuration of a distribution point to support prestaged media. Prestaged media is a new feature of Configuration Manager 2012 and addresses scenarios where administrators would prefer to deliver content in bulk to a distribution point rather than having it copied over the network. In previous versions of Configuration Manager this was not supported natively, although there were tools available to help at least partially address this need, such as PreLoadPkgOnSite.

3. Once you've configured all options on this page as needed, click Next to proceed to the Drive Settings page, shown in Figure 4.41.

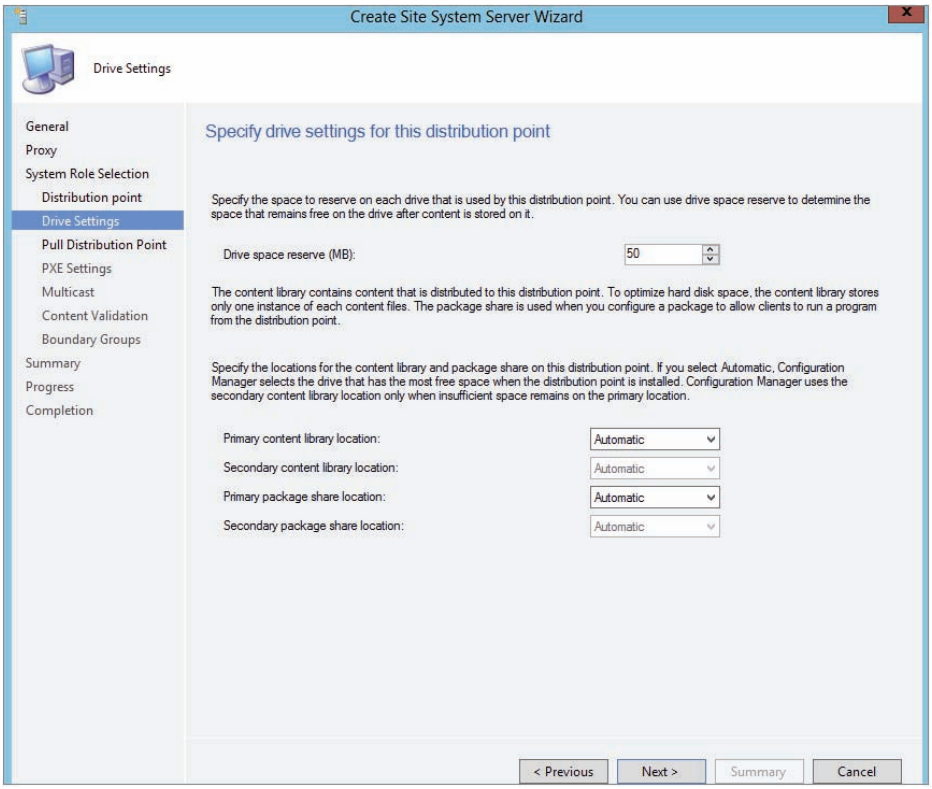


FIGURE 4.41 Create Site System Server Wizard: Drive Settings page

Also new to Configuration Manager 2012 R2 is the ability to control distribution point drive selection and allocate reserved storage when configuring the distribution point. Mechanisms did exist in previous versions of Configuration Manager to make similar configurations effective, notably the use of the `no_sms_on_drive.sms` flag file, but having these options in the console allows more effective and granular administrator control. A couple of options are presented here:

- First is the ability to preconfigure the amount of drive space that should be reserved for the distribution point.
- The next set of options, which are perhaps more important, let you choose which drives should be used for the content libraries and package share locations. In our example, there is only a single drive on the site server, so leaving the options set to Automatic makes sense.

  Also, since there is only a single drive on the server, it doesn't make sense to set a secondary content location, so that option is grayed out. If multiple drives are available and the setting is left at Automatic, then the system will pick the drives to use the same way it has done historically—using the NTFS drive with the most available space as a first choice and so on.

4. Select the Pull Distribution Point page of the wizard if you need this option for your distribution point. The use of pull distribution points can help reduce the processing load on the site server when you deploy content to a large number of distribution points at one site.

   Configure the distribution point to be a pull distribution point by selecting Enable This Distribution Point To Pull Content From Other Distribution Points, as shown in Figure 4.42.

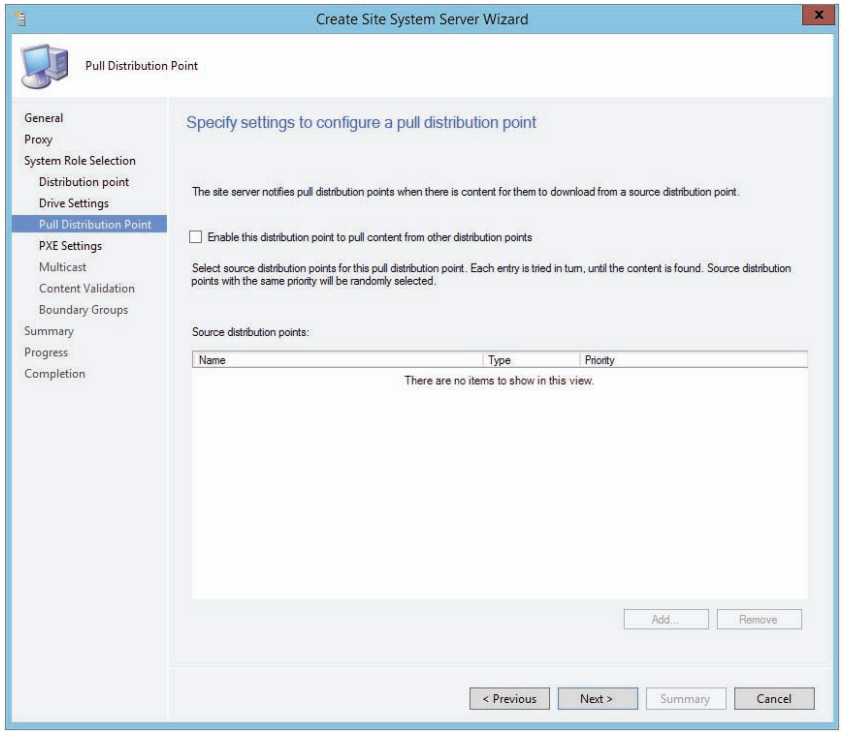


FIGURE 4.42
Create Site System Server Wizard: Pull Distribution Point

- Click Add, and then select one or more of the available distribution points to be source distribution points.
- Click Remove to remove the selected distribution point as a source distribution point.

5. Once the settings are configured as needed, click Next to proceed to the PXE Settings page of the wizard, shown in Figure 4.43.

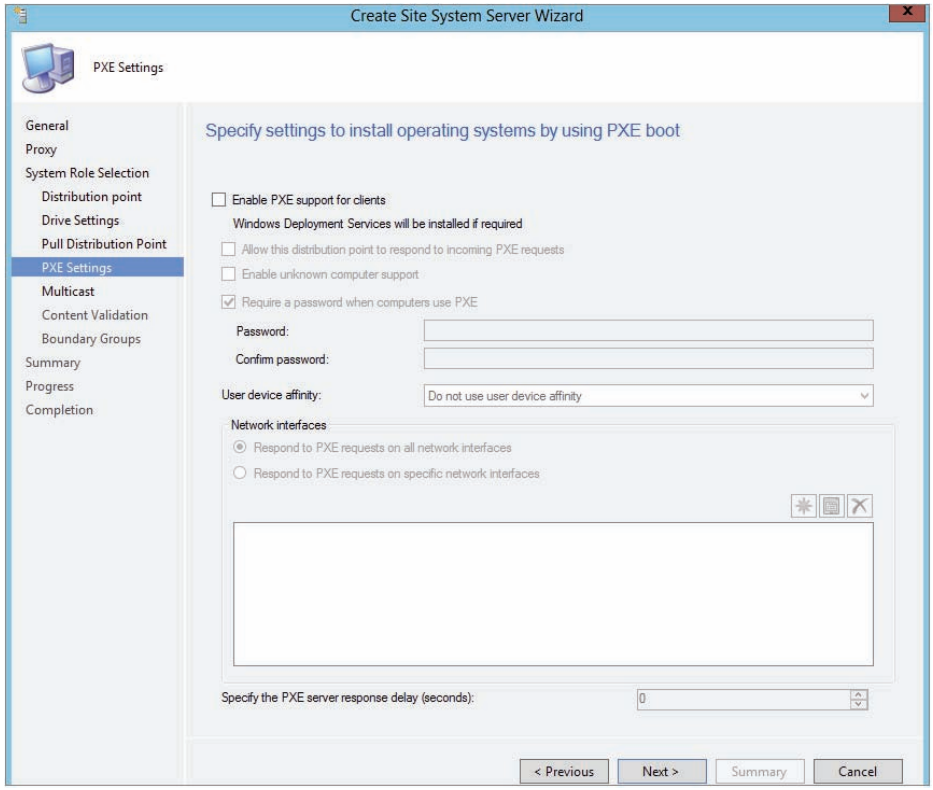


FIGURE 4.43
Create Site System Server Wizard: PXE page

The PXE Settings page of the wizard lets you choose whether the distribution point being configured should also act as a PXE server for operating system deployment. Because of the dependency the PXE server has on the distribution point to deliver boot images, having this setting as part of the distribution point makes sense. For the example we won't install a PXE point; it can be added later as needed.

6. Review the settings on this page and click Next to proceed to the Multicast page of the wizard, shown in Figure 4.44.

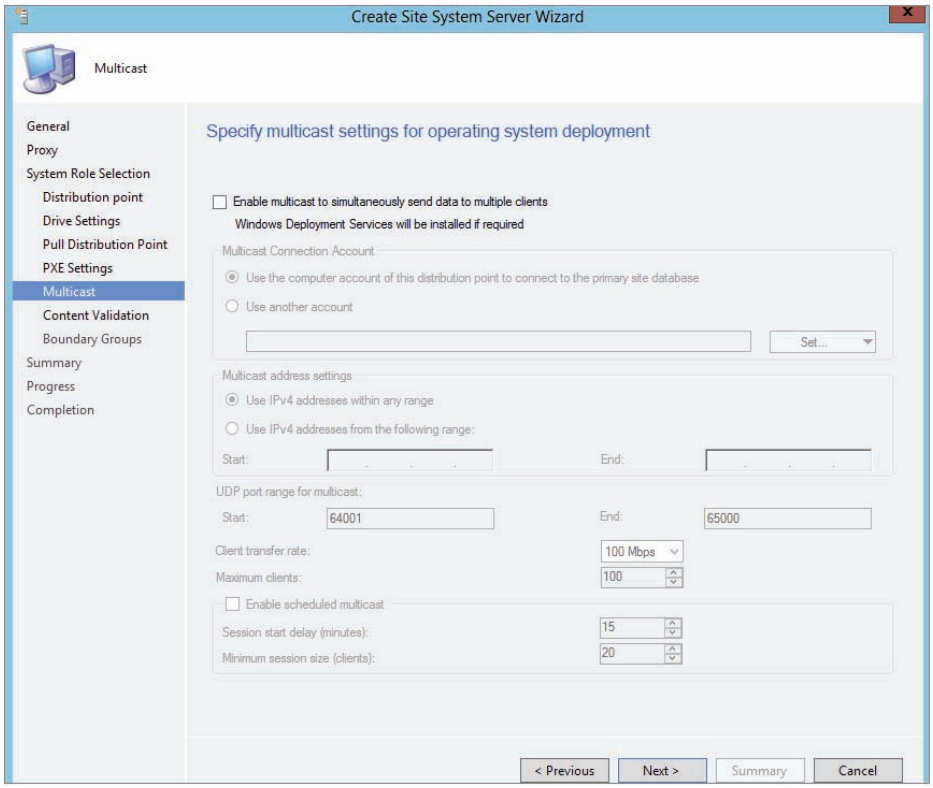


FIGURE 4.44
Create Site System Server Wizard: Multicast page

The Multicast page of the wizard allows administrators to specify whether the distribution point being configured should support multicast or not. Multicast is used with operating system deployment and is a very efficient protocol for delivering images to multiple systems simultaneously. The example distribution point will not be used for multicast support for now, so this option will not be selected. It can be added later as needed.

7. Review the settings on this page, and click Next to proceed to the Content Validation page, shown in Figure 4.45.

   The Content Validation page of the wizard allows administrators to specify whether content should be periodically validated on the distribution point and, if so, on what schedule and at what priority. When Validate Content On A Schedule is selected, the default evaluation period is once per week and at a low priority, to ensure other activities on the server are not disrupted.

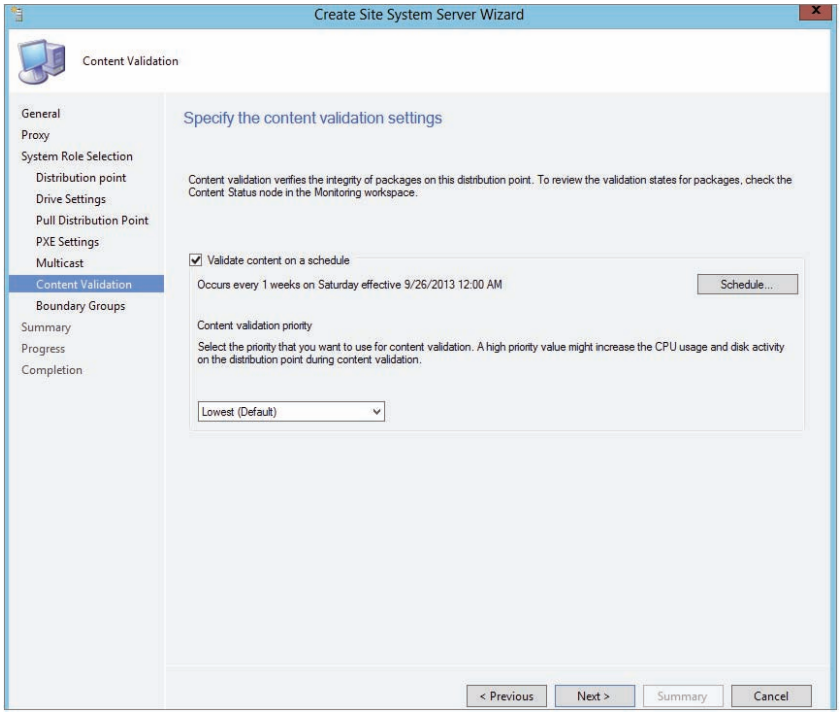


FIGURE 4.45
Create Site System Server Wizard: Content Validation page

This is a significant feature update for Configuration Manager! Most readers who have used distribution points in previous versions of Configuration Manager will have encountered a scenario where content will be distributed to distribution points, work fine for a period of time, and then start to show errors, typically a hash mismatch problem. This might happen for several reasons, often due to on-demand virus scanning of the distribution points, but when encountered, the problem is disruptive until fixed. The ability to do content validation and proactively identify problems is a welcome change indeed! Further, the updated structure of the distribution point should help keep content in a good state as well. More on the distribution point structure shortly.

8. Once you've configured these settings, click Next to proceed to the Boundary Groups page of the wizard, which allows the administrator to choose the boundary group(s) of which the distribution point should be a member. While it is not a strict requirement that a distribution point be a member of any boundary group in order to be created, the distribution point may not be accessible by any client until it is added to the appropriate boundary group(s). Detailed discussion of boundary groups is beyond the focus of this chapter, but based on the tight dependency between distribution point function and boundary groups, a bit of discussion is appropriate here.

   Boundary groups are new in Configuration Manager 2012 R2 and serve two purposes: client assignment and content access. The latter item is the one of concern for distribution point access. We mentioned earlier that on the Create Site System Server Wizard's General page, the option to specify a site system as protected was removed. In Configuration Manager 2012 R2, when a distribution point (or state migration point in operating system

deployment) is added to a boundary group, by definition the distribution point is protected and only those clients that are within the boundaries defined by the boundary group are able to retrieve content from the distribution points that have membership in the boundary group. Further, a distribution point can have membership in multiple boundary groups. By taking this new approach, administrators are afforded additional control to easily specify which distribution points are available to service clients depending on which subnets the clients happen to be located near.

But what if a client requires access to content but is not within boundaries defined by any boundary group, such as a laptop in a hotel room? That scenario is also addressed. Boundary groups can be flagged as accessible to systems when the system is in a location where no other distribution point can be resolved. This is known as *fallback* and is enabled by default for the boundary group, as noted at the bottom of the Boundary Groups page. For the example, the distribution point has been added to a boundary group that was previously created for the example primary site.

9. Once the boundary group configuration is complete, click Next to review the Summary page of the wizard.

10. After confirming all settings, click Next to finish the wizard and implement the distribution point deployment. The successful completion is shown in Figure 4.46.

As mentioned earlier, the Configuration Manager 2012 R2 distribution point structure has changed. After installation is complete and after a couple of applications have been deployed, open the drive hosting the distribution point and check for a few folders, as shown in Figure 4.47.

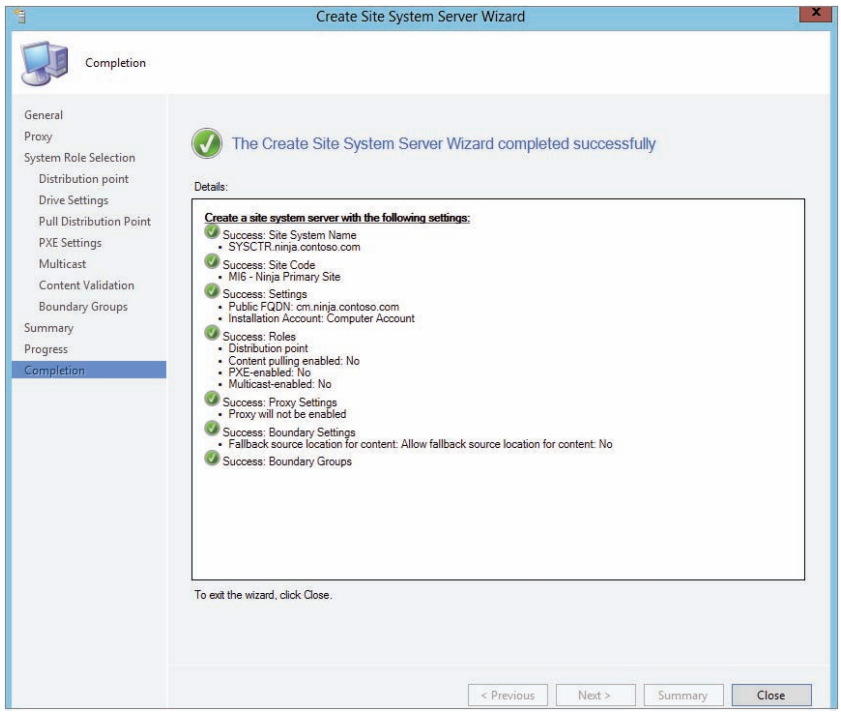


FIGURE 4.46 Create Site System Server Wizard: Completion page

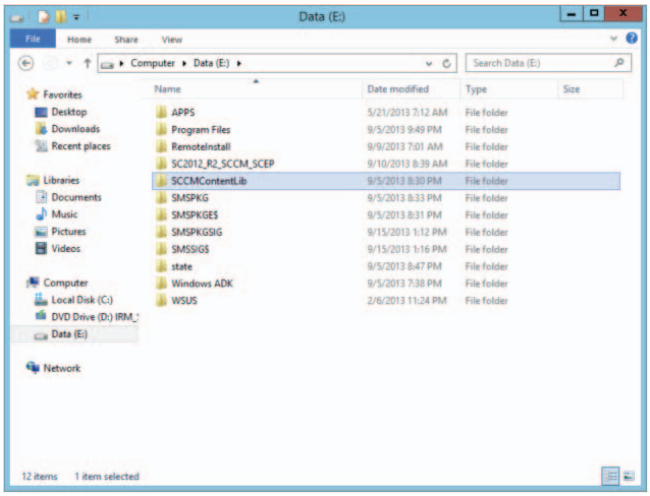


FIGURE 4.47
Distribution point structure

The same folders you might expect from previous versions are still present to support distribution of classic software packages configured to Run From Distribution Point: `SMSPKG`, `SMSPKG<driveletter>$`, `SMSSIG$`, and `SMSPKGSIG`. In addition to these folders another is present called `SCCMContentLib`. This folder contains the new structure for the distribution point and is worth further discussion.

Historically, opening the distribution point folder will reveal a list of folders named with package IDs and, within the folder, the contents of the package. That still is the case, but the structure is far different. Remember that the new distribution point structure in Configuration Manager 2012 R2 is designed to take advantage of single-instance storage and also to be a bit more stable. Looking inside the `SCCMContentLib` folder reveals three additional folders, `DataLib`, `FileLib`, and `PkgLib`, shown in Figure 4.48.

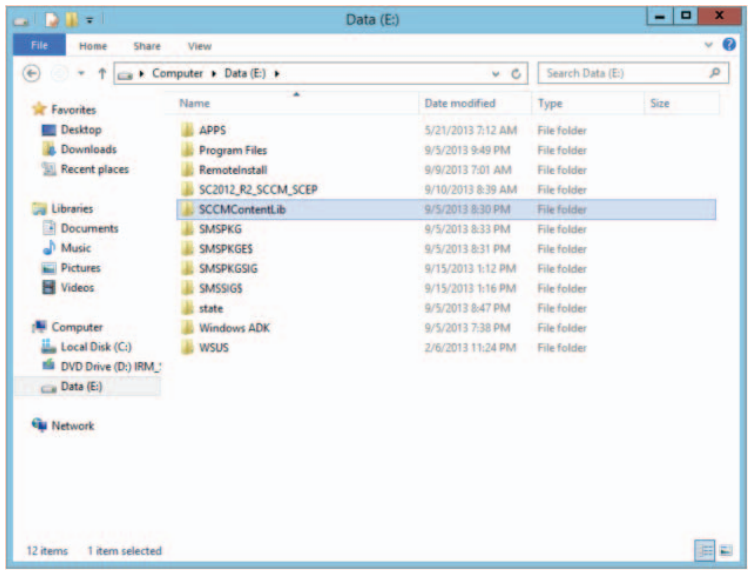


FIGURE 4.48
`SCCMContentLib` structure

The `PkgLib` folder is the starting place to examine the new structure, and it contains files with names that match the package ID from the site, shown in Figure 4.49.

Note that these files are INI files. Looking inside reveals the packages that are associated with the package ID. From here, copy and paste the two `Content_` GUIDs and navigate to the `DataLib` folder, shown in Figure 4.50. For the example, use `Content_3b898e35-9ecc-45e2-9231-ee3f30b2a3aa.1`.

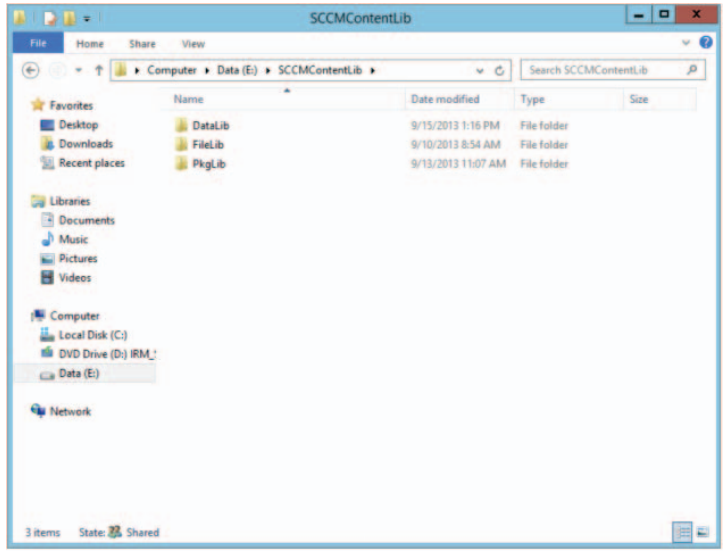


FIGURE 4.49
`PkgLib` folder structure and INI files

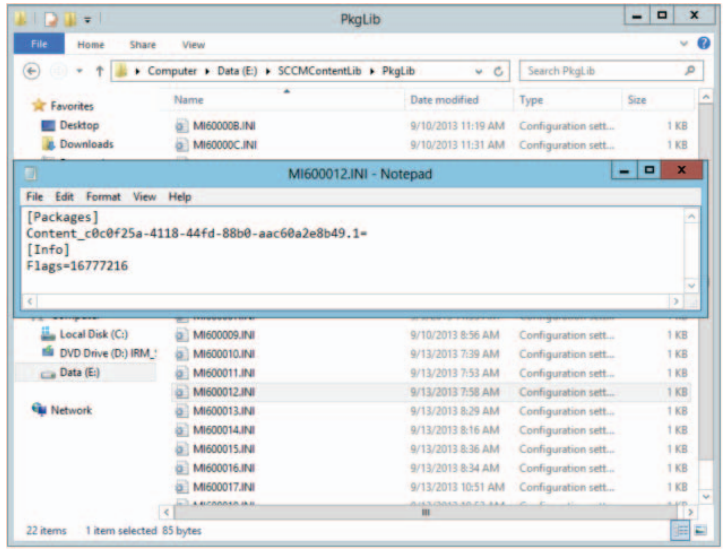


FIGURE 4.50
`DataLib` folder structure, `GUID` folder, and configuration file

In the DataLib folder there are two entries that match; the first is a folder and the second is a configuration file. Looking at the GUID folder first, it looks like the location of the package content. But not so fast! The filenames here will match the filenames from the source file folder, but a quick glance at the file sizes and file extension will show that these are just configuration files. Taking a look at the client.msi file reveals details about the actual file, including file size, in this case 30625792 bytes, and the hash value for the file. The first four characters of the hash value here are key to finding the actual file. In the example, the hash value of interest is 709E. More on this shortly.

In addition to the source file structure there is another configuration file matching the GUID in question; it is at the root of DataLib. Opening it shows a hash value for the folder itself.

Armed with information gained from this folder, it's time to visit the FileLib folder, shown in Figure 4.51.

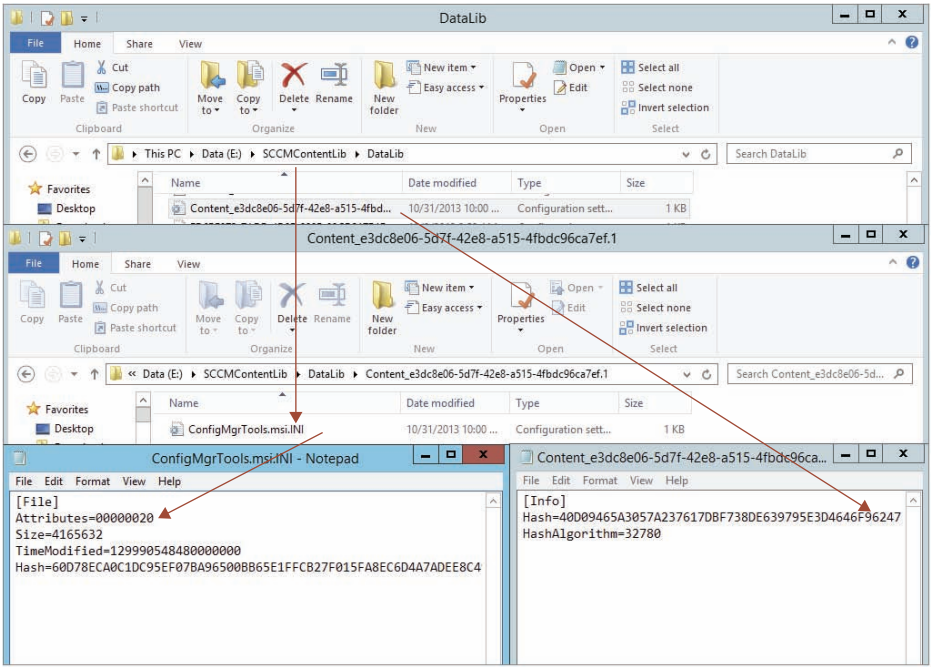


FIGURE 4.51 FileLib folder structure

Within the FileLib folder is a series of other folders with names that at first appear cryptic—only four characters. Aha! Remember that we just mentioned that the first four characters of the hash value for the client.msi file were important. In this folder there is a subfolder named 709E. A quick look inside that folder reveals a file with the exact size of the client.msi file—30,626,792 bytes. Bingo! This is the location of the actual client.msi file, simply renamed and placed into this single-instance storage format.

Software Requirements

Configuration Manager 2012 R2 distribution points require the following:

- All site servers must be members of a Windows 2003 or higher Active Directory domain.
- Distribution points require Background Intelligent Transfer Service (BITS) version 2.0 or higher and cannot be installed or used without it.
- Distribution points may be installed on any supported server or client operating system.
- All Configuration Manager distribution point systems using BITS bandwidth throttling require BITS 2.0 or higher.

Troubleshooting a Configuration Manager 2012 Distribution Point

Without the packages being staged on the distribution points, content deployment (packages, applications, operating systems, and software updates) in the environment cannot be completed. Providing insight into the process and health of the hierarchy distribution points, status messages and log files can be an administrator's best friend.

The Monitoring node of the administrative console, shown in Figure 4.52, will give insight into the health of the distribution points.

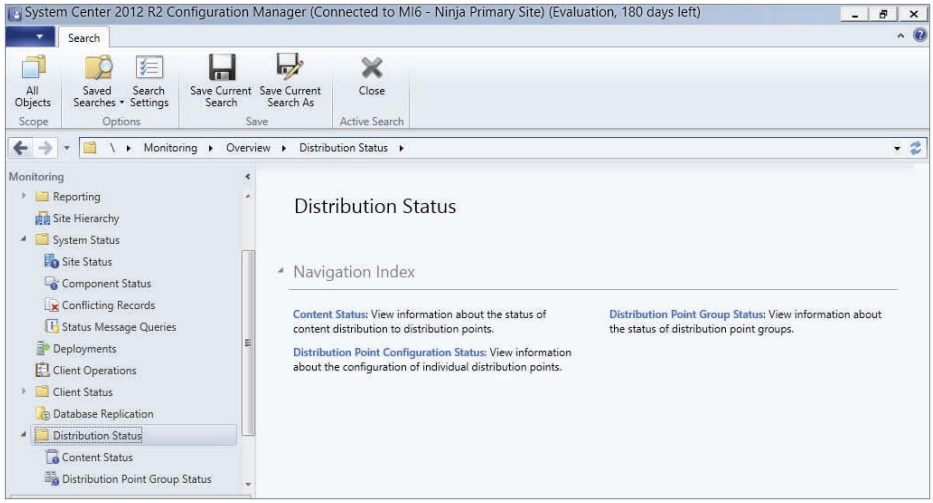


Figure 4.52 Monitoring node, distribution point focus

There is a specific folder for the distribution points, called `Distribution Status`, that provides insight into the status of content, distribution groups, and distribution point configuration. There is also the `Component Status` folder, where you can review the health of `SMS_DISTRIBUTION_MANAGER`, the key component for deploying content to distribution points.

In addition to status messages, `distmgr.log` provides insight into the distribution points for troubleshooting purposes. It tracks the different packages by package ID, size, and location where they are to be stored.

Management Point

A *management point* is the primary point of contact between the Configuration Manager 2012 R2 clients and the site server. All site servers that host clients must have at least one management point installed; this includes primary site servers and secondary site servers. A management point installed at a secondary site server is known as a proxy management point. Clients use the management point to retrieve and send all data to and from their assigned site server; this includes retrieving settings and configuration via the policy and forwarding operational data such as inventory, state messages, status messages, discovery information, and more. In addition, clients will send requests to the management point requesting help locating content they may need, such as finding which distribution points are available to the client and contain needed software update or software package content or even the location of a software update point used in software update scanning.

Once a management point receives data from the client, it will be further analyzed and converted into a form acceptable by the site server and then forwarded to the site server for further processing. This also includes content location requests, but in these cases there is no data to forward to the site server. Instead, the management point will execute queries against the site database and return that information to requesting clients.

Here are a few things to remember about management points:

- Every primary and secondary site must have a management point specified.
- The Central Administration Site cannot host a management point.
- Management points require access to the site database for certain operations.
- Management points require a local installation of IIS to be installed.
- Management points make use of BITS when moving content, depending on size, to help avoid impacting network utilization.

Also of interest for management points is that they no longer have a dependency on WebDAV. Add to this that management points are now treated similarly to distribution points in that they can be placed where needed to support clients. In previous releases of Configuration Manager, the only way to host multiple active management points at a site was by using a network load balancer as a front end. Now management points are simply looked up by clients—similar to distribution points—and the best choice at a site is returned to the client. This statement may cause you to ask how exactly clients learn about possible management points. There are a couple of ways. It's possible to specify a single or multiple management points on the command line when installing the client using the SMSMP switch. If Active Directory publishing is enabled, then clients will be able to look up the management point list from there as well. During client installation, and during ongoing client operation, they will learn which management point is optimum for their use through boundary groups—again, much the same as distribution points.

Another big shift for management points is that now the server locator point functionality is included in this role.

It may be that the management point role is already installed. One of the default settings when installing a primary or secondary site is to also add the management point role. If the role was not yet added as part of setup, then you will need to add it.

1. In the Add Site System Roles Wizard, select to add the management point role, and click Next to proceed to the Management Point page, as shown in Figure 4.53.

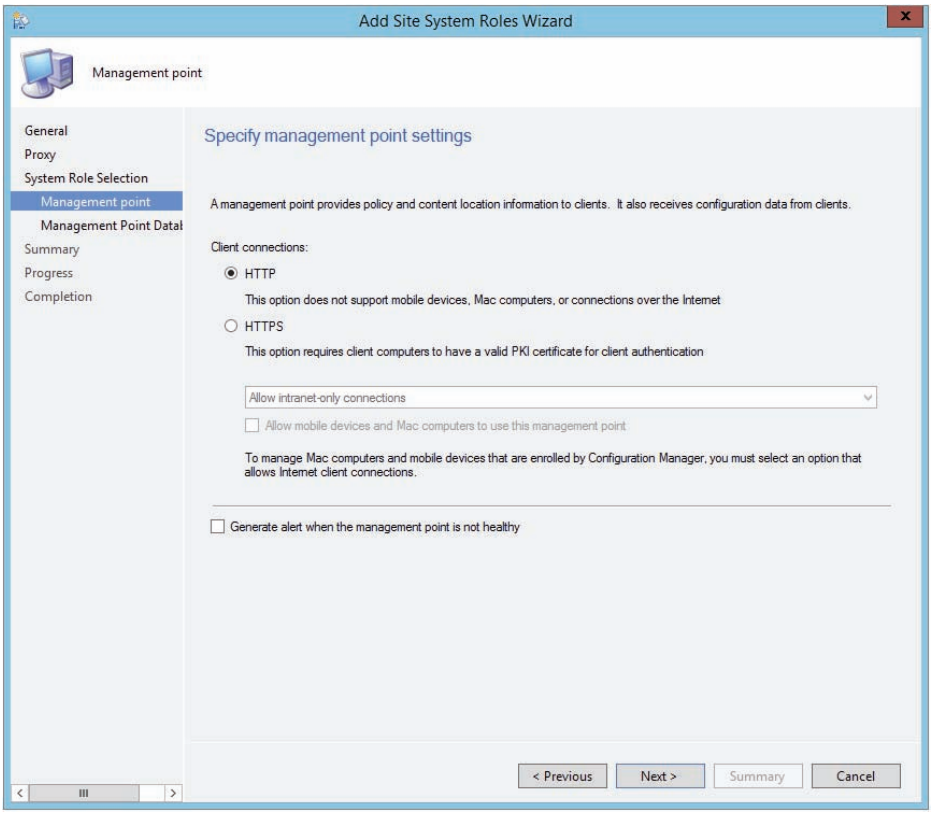


FIGURE 4.53
Add Site System Roles Wizard: Management Point page

- The first choice on this page allows administrators to choose how clients should communicate with this management point, either by HTTP or by HTTPS.
- Administrators are also able to specify whether they want to receive an alert in the console indicating when the management point is unhealthy.

  This is a new option for Configuration Manager 2012 R2, and it points to the basic monitoring capability that has been added. If this option is selected, administrators can find alerts generated in the Monitoring workspace of the console.

2. Click Next to continue to the Management Point Database page shown in Figure 4.54.

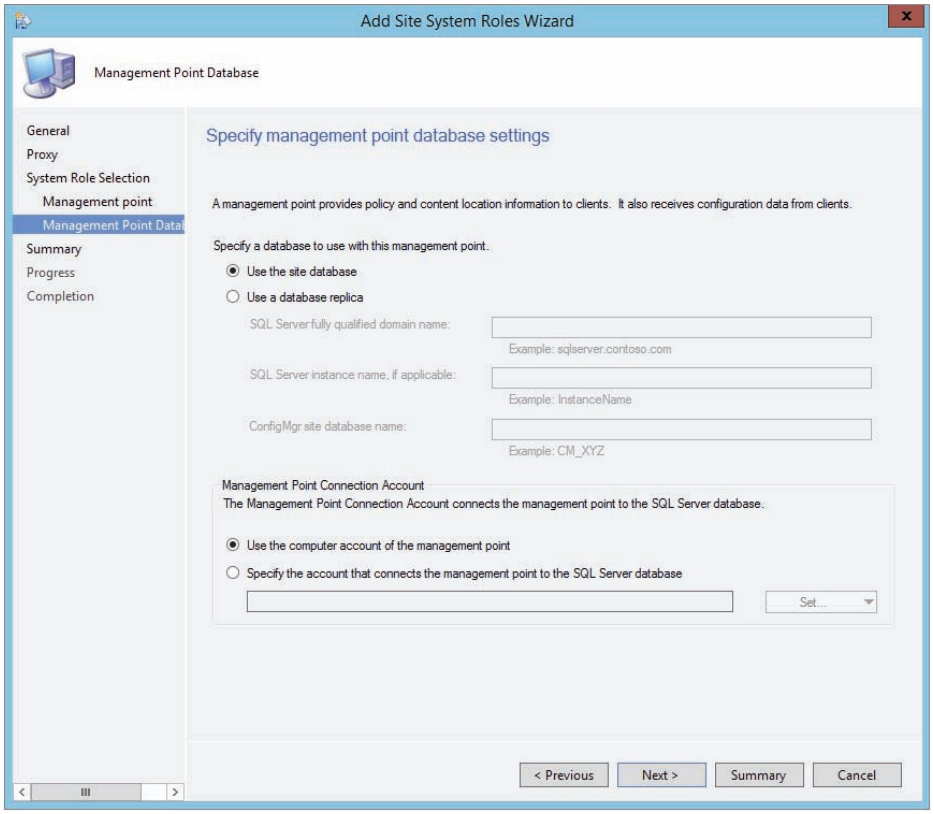


Figure 4.54
Add Site System Roles Wizard: Management Point Database page

Proxy Management Points

Proxy management points are the same as standard management points except that they are located at a secondary site. In previous versions of Configuration Manager it was the administrator's choice whether to include a proxy management point at secondary sites. In Configuration Manager 2012 R2 there is no choice; proxy management points are automatically installed on every secondary site server.

Proxy management points exist to help reduce the impact on the WAN when clients are operating outside the boundaries of their assigned primary site but within the boundaries of a secondary site that is a child of their assigned primary site. A client in this configuration will consider the proxy management point to be its local management point but will always consider the management point from its assigned primary site to be the assigned management point. The difference between the two is that the client is able to use the local management point to find local distribution points via content location requests and also as a point for offloading data, such as inventory and state messages, on its way to the parent site's database. The client will still use its assigned management point to retrieve all policy changes.

Proxy management points can significantly reduce the load on WAN traffic by processing data from and providing client policy to those clients that fall within their roaming boundaries. Data flow between Configuration Manager clients and the Configuration Manager 2012 R2 hierarchy is as follows:

1. Clients send discovery data, inventory data, status data, and software-metering data to the proxy management point in XML format.
2. The proxy management point processes the submitted XML file and converts it into the appropriate file type, and the file is placed in the associated `Inbox` directory on the secondary site server.
3. The secondary site server processes the data as it would under normal circumstances and forwards it up the hierarchy to its parent site.

Proxy management points also retrieve policy information from the database of the primary site and forward the data to Configuration Manager clients. Proxy management points allow the client to function locally when roaming to a secondary site, while further allowing administrators to control the replication of client data from the secondary site to the primary parent by means of standard sender throttling.

How Clients Find Management Points

During installation and general operation, Configuration Manager 2012 clients obtain management point locations in much the same way as they look up distribution points. Configuration Manager 2012 R2 allows for multiple active management points per site. Periodically, clients will poll for which management point they should be using. The determination is made by evaluating boundary groups in relation to the client, very similar to the mechanism used to find distribution points. If a client roams outside of its assigned sites boundaries, then the lookup is a bit more complex but is needed to allow clients to access local management point servers where possible. There is also a lookup mechanism for management points in Active Directory.

Locating Management Points in AD

In an environment that provides Active Directory services, Configuration Manager 2012 R2 clients locate management points as follows:

1. The client searches the Active Directory global catalog for a local site code with a matching Active Directory site name, IP network, or IP address range that has been previously registered by a site server.
2. If a match is not found or if required content is not available at the local site, then the client uses the site code of its assigned site.
3. The client then queries Active Directory again to find the appropriate management point for the site code identified in the previous steps.

   For this reason, management points should be installed prior to Configuration Manager client deployment, but the client will be able to access the management point once it becomes available.
4. If there is only one management point for the site, the client gets the name of that management point from Active Directory and then connects to it.

Overlapping Boundaries and Management Point Location

The fact that the client will always query Active Directory first when attempting to locate management points is one of many reasons why overlapping site boundaries is unsupported and will wreak havoc on an environment. When sites publish their information to Active Directory and that information is inconsistent, as in the case of overlaps, the client may not choose the correct management points for use when looking up content locations. The result may be failed software deployment in the environment, not to mention the implications for proper client assignment if installing clients.

Automatic MP Query

When installing the Configuration Manager client, you must either set it to determine the SMS site automatically or specify site assignment as part of the command line for the installation. During installation and after being assigned to a site, the client will look up the appropriate management point it should be using. The client gets this list either by command line during installation, querying active directory, or learning about additional management points and adjusting after installation.

In addition, a new option has been added to Configuration Manager 2012 R2 to specify a default site a client should be assigned to if it is unable to find a site by normal lookup mechanisms. This fallback ability helps ensure clients do not get installed and immediately orphaned because they cannot find a site.

You can see this in the `LocationServices.Log` file of the Configuration Manager client, located at `%Windir%\CCM\Logs`.

Server Locator Point functionality

As mentioned, the server locator point functionality has been merged into the management point role. But what is a server locator point used for? Server locator points are used within a Configuration Manager 2012 hierarchy to provide services for client site assignment, location of client installation files, and location of management points when clients cannot access that information within Active Directory. Thus, merging this role with the management point role is a natural fit.

Logging

Logs of management point activity can exist in one of two locations, depending on which was installed first: the Configuration Manager client or the management point. The management point and the client share a common framework and thus both run under the SMS Agent Host service or the short name of CCMExec. This is potentially confusing at first because it is possible to have just a management point installed without the client component, but the service name will still be SMS Agent Host.

If the management point is installed on a server first, the logs will be located in the `.\SMS_CCM\Logs` directory. When the Configuration Manager client has already been installed on the server, the logs are located in the `%Windir%\CCM\Logs` directory along with the client-side logs.

Default logging is good for both the client and the management point, but there are some log details that won't be seen unless verbose and debug logging are enabled. Some of the information that is accessible with this extra level of logging is so useful that it is common practice to configure verbose and debug logging as a standard across the environment. There is additional overhead because more data is written to the logs, but it is minimal and should cause no impact to the operation of the system.

Enabling verbose and debug logging requires two registry changes. First, you enable verbose logging by navigating to

```
[HKEY_LOCAL_MACHINE\software\microsoft\ccm\logging\@global]
```

and changing the value LogLevel to 0 (which will require a permissions change on the `@GLOBAL` key). To enable debug logging, create a registry key called `DebugLogging` directly under

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Logging]
```

Inside this registry key create a string value named Enabled and set its value to True.

Software Requirements

Configuration Manager 2012 R2 management points require the following:

- All site servers must be members of a Windows 2003 or higher Active Directory domain.
- IIS 6.0 or higher must be installed.

Troubleshooting a Configuration Manager 2012 R2 Management Point

The Configuration Manager management point is the entry point into a Configuration Manager hierarchy from a client perspective. The client receives its Configuration Manager policies and advertisements from the MP and places its inventories and status there. As with all components, administrators have a choice of using status messages and/or log files to verify management point function.

You can view management point status in the Monitoring node of the console by checking components such as `SMS_MP_CONTROL_MANAGER` or `SMS_MP_FILE_DISPATCH_MANAGER`. If you prefer using logs, then the following logs are key to verifying proper management point installation and function:

`mpMSI.log` This is the Microsoft Installer (MSI) log for the management point installation.

`mpSetup.log` This is the site-specific management point log, which shows which site and server the management point is configured to use.

`mpcontrol.log` This log maintains the management point by reviewing and checking the management point availability and status.

Site Database Server

Every Configuration Manager 2012 R2 implementation will have at least one server running the site database server role. The simplest implementation will have a single server running all the Configuration Manager 2012 R2 roles as well as Microsoft SQL Server 2008 Service Pack 1 or higher. As noted earlier, at least one database repository is required to store all the client information and site configurations.

A Configuration Manager 2012 R2 site database server requires the following:

- All site servers must be members of a Windows 2003 or higher Active Directory domain.
- Microsoft SQL Server 2008 Service Pack 1 or higher is the only version of SQL Server supported for hosting the Configuration Manager 2012 R2 database. (There may also be Cumulative Update requirements; for the latest list, check the TechNet documentation.)
- The SQL database service is the only SQL Server component required to be installed to host the site database.

Troubleshooting a Configuration Manager Site Database Server

This is the database server that hosts the Microsoft SQL Server 2008 Service Pack 1 database. There is one database that holds all information about inventory, packages, status, and all the other pertinent data of System Center Configuration Manager 2012 R2. The following logs provide insight into the health of the database server:

`smsdbmon.log` This log shows all activities such as inserts, updates, drops, and deletes from the Configuration Manager 2012 R2 database.

`smsprov.log` This log shows the SQL transaction calls made from the Configuration Manager console or automation scripts via the SDK.

Site Server

A *site server* is a unique site system role in Configuration Manager. This role cannot be manually added, nor can it be manually removed. This role is managed by the site server itself and will exist on any server that is serving as a site server in the hierarchy. When a site is installed, whether a Central Administration Site, primary site, or secondary site, it will be shown as having the site server role.

This role manages all functions of the site and interacts with all remote systems hosting site system roles for the site. The overall health of the site server role can be reviewed in the Monitoring node of the console and also by examining the site server logs generated.

Site System

A *site system* is a unique site system role in Configuration Manager. This role cannot be manually added nor can it be manually removed. This role is managed by the site server itself and will exist on any server that is serving as a site system in the hierarchy. The site server itself will always be a site system as will any remote servers that are deployed to host various roles to provide services needed by the site.

The overall health of the site system server can be reviewed in the Monitoring node of the console. The specific nodes to review as well as the specific log files will be dictated by the specific functions being performed by the site system server.

System Health Validator Point

The system health validator point is the Configuration Manager 2012 R2 site system role that runs on Windows Server 2008 and Windows 2008 R2 servers with the Network Policy Server role enabled. Network Policy Servers evaluate clients as they attempt to come on the

network and either grant access or deny access depending on whether clients comply with configured policy. The system health validator point is the Configuration Manager add-on to the Network Policy Server that provides the ability to judge whether a given client complies with required patch levels.

In brief,

1. Client health state evaluation proceeds by the client producing a statement of health locally and sending this to the Network Policy Server.
2. When received, the statement of health is evaluated against configured conditions and a resulting client health state is determined. The state may be
   - Compliant, resulting in network access
   - Noncompliant, resulting in network access being denied until the detected problem is remediated

An error condition may be returned that prevents evaluation.

The system health validator point validates a statement of health using a sequential series of checks. These include the following:

- Time validation when the statement of health was created
- Validation against the health state reference
- Compliance status and failures

The system health validator point never communicates directly with Configuration Manager 2012 R2 site servers to validate client statements of health. When a Configuration Manager Network Access Policy is created or modified or inherited from a parent site, the site server writes a health state reference to Active Directory Domain Services. The system health validator point periodically retrieves the health state references for all Configuration Manager primary sites that are enabled for Network Access Protection (NAP).

Because Active Directory Domain Services is used to store the health state references, the Active Directory schema must be extended with the Configuration Manager 2012 R2 extensions. The health state reference is published to a System Management container in Active Directory, which requires that Configuration Manager 2012 R2 publish site information to Active Directory Domain Services. When there is more than one Active Directory forest and your Configuration Manager site servers and system health validator points are not in the same forest, you must designate which forest and domain will store the health state references.

If the system health validator point role has not yet been added, it will need to be selected. Until now components have been installed on just the site server system. In production it is unlikely that the site server will also act as a Network Policy server, so configuring this role will likely require creating a new site system server to host the role. The new site system server should be the server hosting the Network Policy server components in the environment.

1. In the Add Site System Roles Wizard select to add the System Health Validator point role.
2. Click Next to proceed to the System Health Validator page of the wizard. There are no properties to configure on this page.
3. Simply complete the wizard to install the component.

Software Requirements

Configuration Manager 2012 R2 system health validator points require that all site servers be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting a Configuration Manager 2012 R2 System Health Validator Point

Within the entire Network Access Protection scenario, this role allows the infrastructure to validate the statement of health from a NAP-capable Configuration Manager client. For troubleshooting, use the `SMSSHVSetup.log` file, which documents the prerequisite and installation progress.

State Migration Point

Think of the state migration point role as a reverse distribution point. The state migration point is a Configuration Manager site system role that provides a secure location to store user state information as part of an operating system deployment. User state is stored on the state migration point while the operating system deployment proceeds and is then restored from the state migration point to the new computer at the appropriate time during imaging. Each state migration point site server can be a member of only one Configuration Manager 2012 R2 site, but each site may have multiple state migration points if needed.

If the state migration point role has not yet been added, you will need to select it, as shown in Figure 4.54.

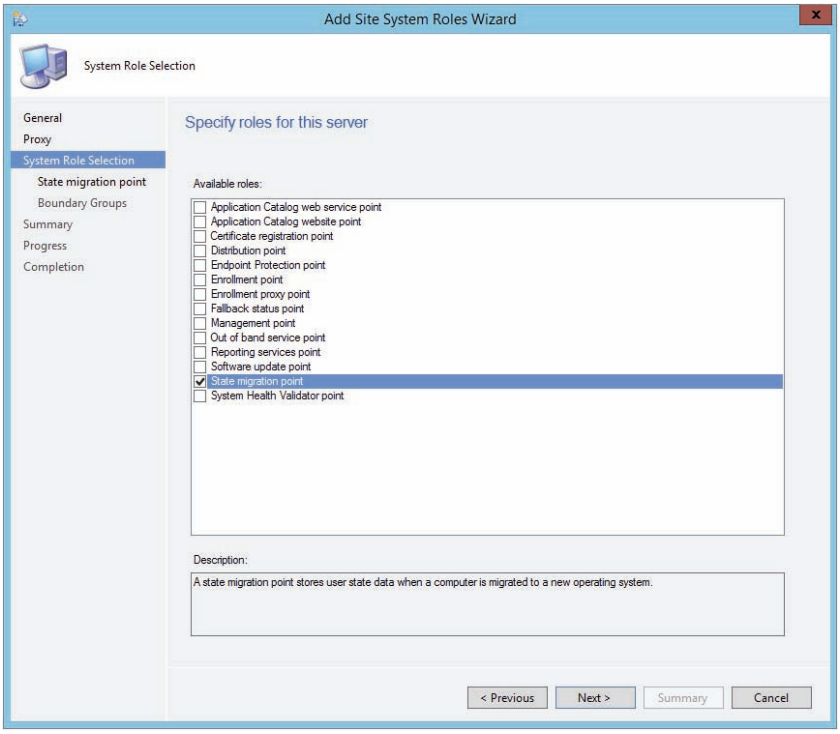


Figure 4.55 Add Site System Roles Wizard: State migration point selected

1. Choose the site where the state migration point will be located, and select the role in the Add Site System Roles Wizard.
2. Click Next to proceed to the State Migration Point page of the wizard, shown in Figure 4.55.

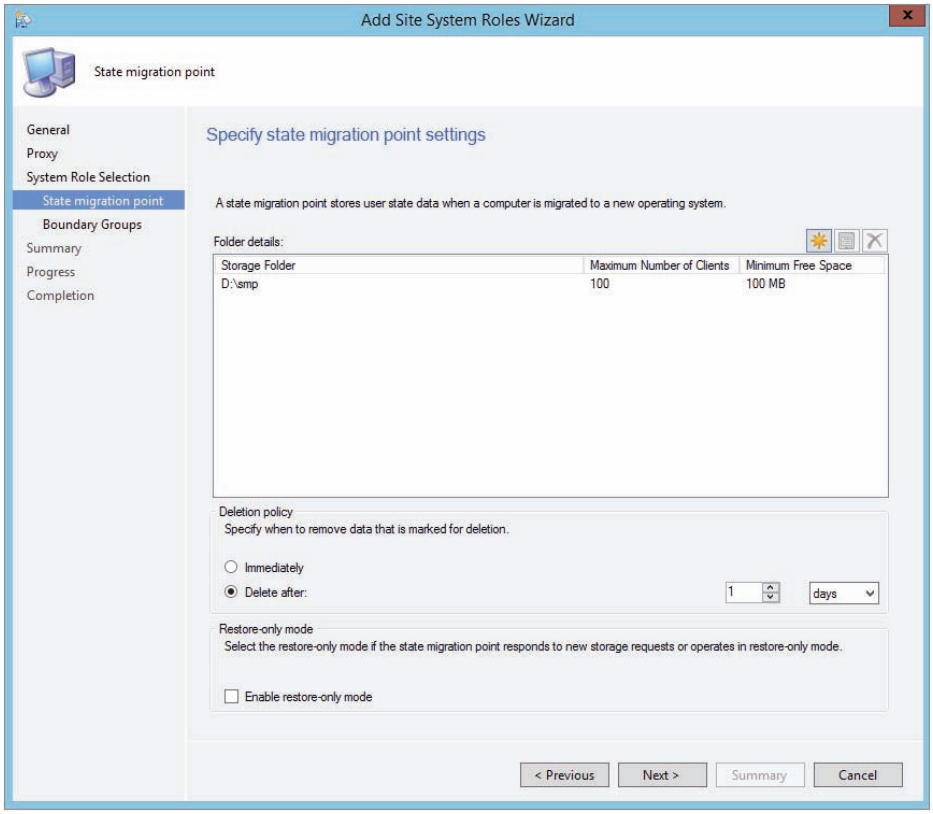


FIGURE 4.56
Add Site System Roles Wizard: State Migration Point page

This page allows configuration of the state migration point.

3. First, choose the folder that will host user data sent to the state migration point.

   This includes choosing the drive, the folder name, the maximum number of clients that may be served by the state migration point, and also the minimum amount of disk space that should be reserved.

4. Configure the Deletion Policy to show how long user state data is held following a successful operating system deployment before being deleted.

This raises an important point. When user state data is stored on the state migration point, it is with the intention that the state data will be restored to either the same system or a different system as imaging nears completion. If the state data is never restored, it is never marked as eligible for deletion because there might have been problems during the imaging process, and allowing deletion would remove potentially needed data from the system. This is particularly true if the deletion settings specify to remove data immediately.

5. Finally, flag the state migration point as being in restore-only mode.

   This special setting, disabled by default, allows administrators to configure a state migration point so that it doesn't receive new state data but is available for use in already stored state data. Typically you would set this option if you have a state migration point server that is scheduled for maintenance or replacement; you could also use this option if you are building a new state migration point but you don't want it to go into service yet.

6. Once the configuration settings are complete, click Next to proceed to the Boundary Groups page of the wizard, shown in Figure 4.57.

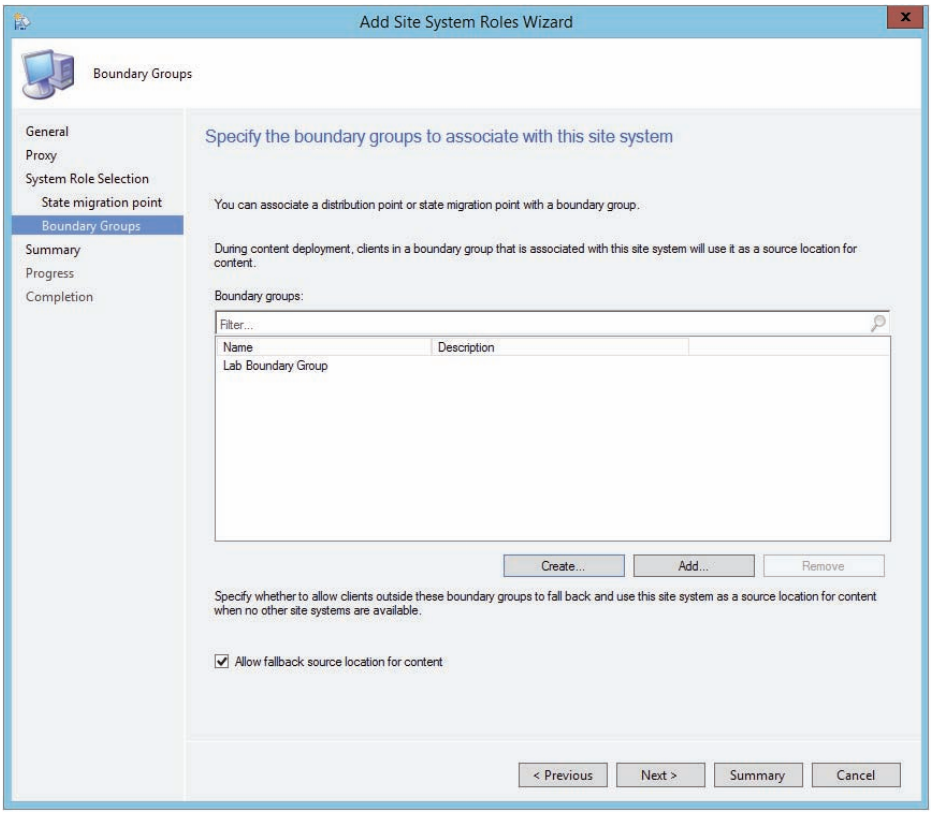


FIGURE 4.57 Add Site System Roles Wizard: Boundary Groups page

Like the distribution point, the state migration point needs to be added to an appropriate boundary group to make it available for use by clients. If the state migration point is being installed on a server that already hosts the distribution point role, then the boundary group may be prepopulated.

7. Make any needed changes and click Next to continue through the wizard and finish up.

Software Requirements

Configuration Manager 2012 R2 state migration points must be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting a Configuration Manager 2012 R2 State Migration Point

This role is leveraged during the operating system deployment. In particular, it is used to store user data for migration back onto their machine that was just reimaged or replaced. The health of the state migration point is visible in the Monitoring node of the console and also by reviewing the following logs:

`smssmpsetup.log` This log documents the appropriate prerequisites and logs the initialization of the `smp.msi` file and installation completion.

`smpmsi.log` This log documents the installation setup progress of the `smp.msi` file.

Fallback Status Point

The fallback status point role helps address today's greater security requirements while enabling a mechanism to catch clients that are not communicating properly. When deploying clients it is critical to know if problems are being encountered. Typically these problems are reported to the management point in the form of status or state messages. When installing the client, there is a time when it is not possible to send data to the management point. In addition, there may be problems reaching the management point even after install. In such cases, if the client does not have a mechanism to notify the site of problems, it will become orphaned and unusable. The fallback status point role provides an administrator with insight into the installation and management of a client and works well because the location of the fallback status point is configurable on the command line when client installation is initiated.

A fallback status point is similar to a proxy server that proxies client status messages up to the site server. Two types of messages may occur: the normal messages that appear during client installation and assignment or those identifying unhealthy Configuration Manager 2012 R2 clients. In either scenario, the fallback status point fills the gap and shows the administrator that there are client issues that need to be addressed.

Because of the potential security threat of an unknown client or client status, it is recommended that the fallback status point be placed outside a physical site server. It can be a low-end server, because of the relatively small number of potential requests it should receive. As in any design decision, the criteria of scale versus risk should be investigated before a decision is made.

Through detailed reporting, an administrator can gain knowledge and take proactive measures to ensure that availability remains in its highest state. These reports include detailed client information on capable and incapable client communication.

Installation of a fallback status point is not a requirement for a site but it is recommended. Typically there is one fallback status point installed per site that hosts clients.

If the fallback status point role has not yet been added, you will need to select it.

1. Choose the site where the fallback status point will be located, and select the status point in the Add Site System Roles Wizard.
2. Click Next to proceed to the Fallback Status Point page of the wizard, shown in Figure 4.58.

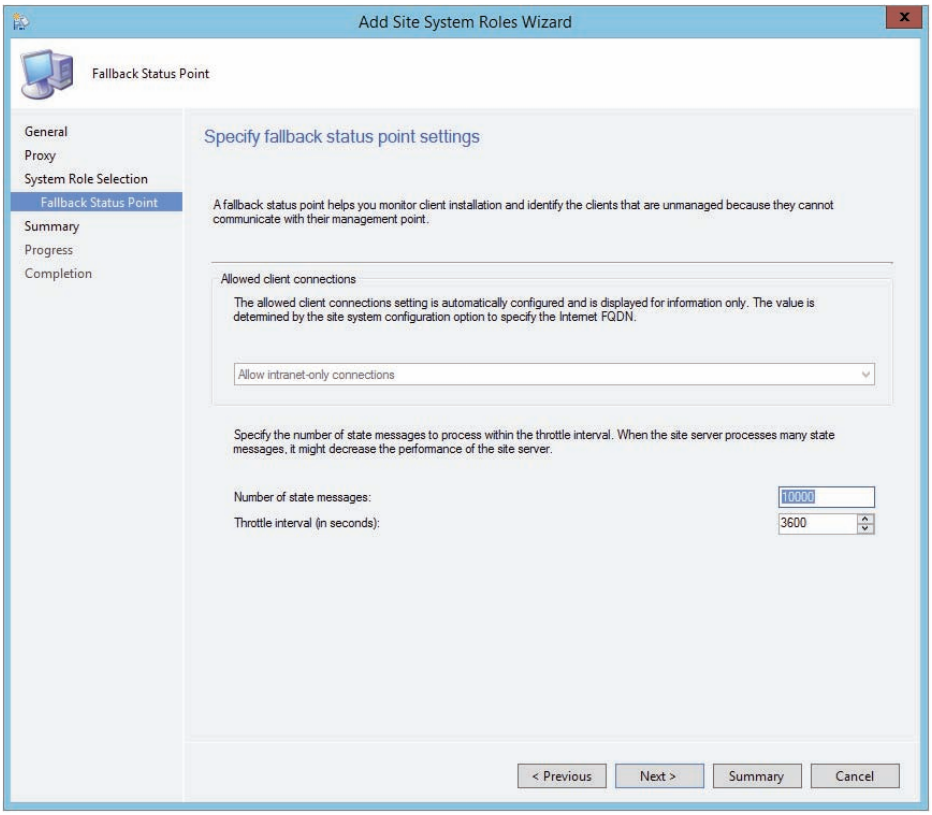


Figure 4.58 Add Site System Roles Wizard: Fallback Status Point page

There is little configuration to be done for the fallback status point. The only option is to configure the number of state messages that are allowed to be processed during the given time window. Typically the default values are fine.

3. Make any needed changes, and click Next to complete the wizard.

Software Requirements

Configuration Manager 2012 R2 fallback status points require that all site servers be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting the Fallback Status Point

The fallback status point is meant for clients that are having difficulties communicating with a Native mode Configuration Manager hierarchy. To provide insights into the proper configuration of this role, the component status is available in the Monitoring node of the console and also by reviewing the following logs:

SMSFSPSetup.log This log documents the prerequisites and kicks off the `fsp.msi` installation.

fspMSI.log This log provides the installation status of the fallback status point role.

Out of Band Service Point

The out of band service point is the site system role that serves as the management interface between Configuration Manager and client systems that are operating with Intel's Active Management Technology (AMT) vPro chipset, a technology available in workstation-class systems.

Intel is the first hardware vendor to provide direct hardware interactions to leverage Windows Remote Management capabilities. These capabilities include remote boot control, forced PXE boots, remote network boots, and direct inspection of the hardware inventory and power state. AMT is even able to wake a machine from sleep state if needed! A goal of this technology is to empower full system management without the expense of desktop visits. These capabilities become very attractive when addressing geographically dispersed branch offices where there is little or no support staff to physically remediate workstations. Since Configuration Manager is the world-class systems management suite, the inclusion of AMT as a capability just makes sense.

Before a system is able to be managed, it must be *provisioned*. In Configuration Manager 2007, a provisioning process known as out-of-band provision was supported, a process that allowed a workstation to be configured even without an installed operating system. Configuration Manager 2012 R2 supports in-band provisioning only—meaning that a Configuration Manager 2012 R2 client needs to be installed and assigned to a site. Provisioning also requires the use of certificates. The out of band service point is the focus of activity during provisioning because it connects to and interacts with AMT-capable systems.

Setting up Configuration Manager/AMT integration and management requires several steps. One of the first steps in the process is to install an out of band service point. One out of band service point will be needed at each primary site that provides AMT management. If the role has not yet been added, you will need to select it in the Add Site System Roles Wizard.

1. Choose the site where the out of band service point will be located, and select the service point in the Add Site System Roles Wizard.
2. Click Next to proceed to the AMT Service Point page of the wizard, shown in Figure 4.59.
3. On the AMT Service Point page, configure the number of retry attempts that should be made, along with the delay between retries, when attempting to connect to an unresponsive AMT system.

   You can also specify the maximum number of transmission threads between the out of band service point and AMT-equipped systems on this page. If AMT is heavily utilized, it may be appropriate to change the default settings. If you make changes, however, take care to ensure the performance of the host system is not adversely affected.

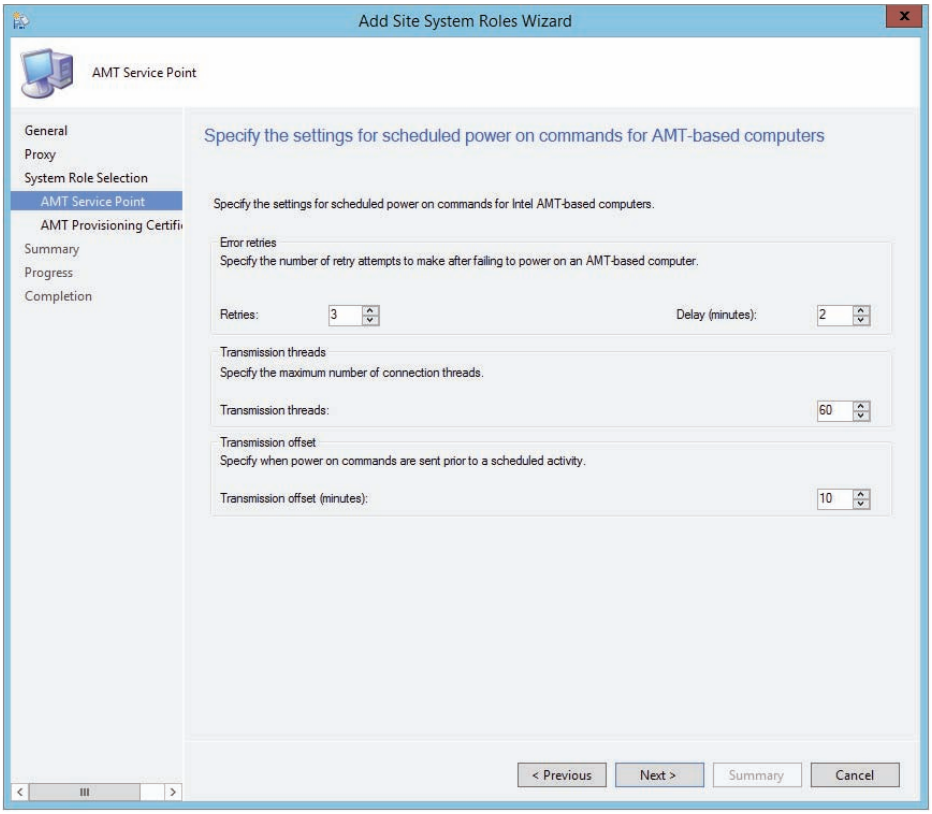


FIGURE 4.59
Add Site System Roles Wizard: AMT Service Point page

The transmission offset is the last setting on this page and defines how long before any scheduled activity, such as scheduled software distribution, an AMT system wake-up command should be sent. This is an important feature of AMT and should be considered along with Configuration Manager Wake On LAN capabilities.

4. Adjust configurations as needed, and click Next to proceed to the AMT Provisioning Certificate page, shown in Figure 4.60.

5. On the AMT Provisioning Certificate page, browse to the provisioning certificate that will be used and import it.

   A provisioning certificate will be used for validation when connecting to AMT-enabled systems and initializing the provisioning process.

6. Choose whether to enable CRL checking for the AMT provisioning certificate, and then click Next.

Configuration Manager 2012 R2 out of band service points require that all site servers must be members of a Windows 2003 or higher Active Directory domain.

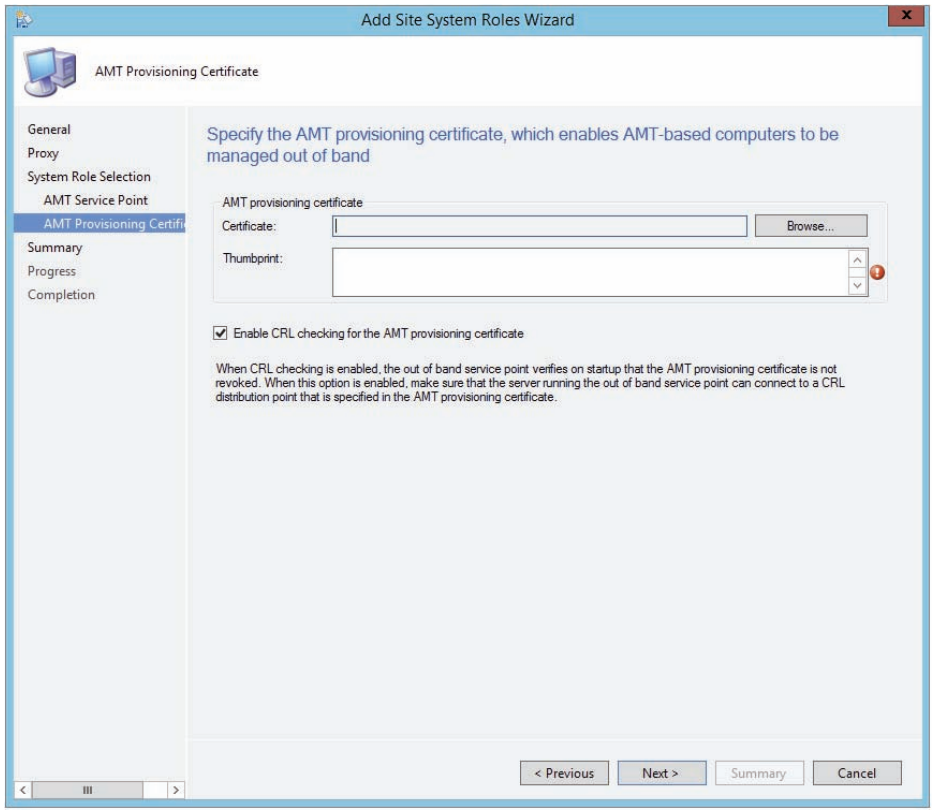


FIGURE 4.60
Add Site System Roles Wizard: AMT Provisioning Certificate page

Reporting Services Point

The Reporting Services point provides integration between Configuration Manager and SQL Server Reporting Services (SSRS) to facilitate report publishing and rendering. This is a big change in Configuration Manager 2012 R2; the reporting engine available in previous versions of Configuration Manager, classic reporting, is gone. SSRS integration was first introduced in Configuration Manager 2007 R2 and was available in parallel to classic reporting, providing customers time to adjust to the new (and long overdue!) approach to reporting.

SSRS integration just makes sense. Most people don't enjoy reading through line after line of tabular reports and would prefer to encapsulate that same data in a graphical format. SSRS can handle most any reporting scenario with ease.

If the SSRS role has not yet been added, you will need to select it in the Add Site System Roles Wizard.

1. Choose the site and server where the Reporting Services point will be located.

   If a Central Administration Site is in place, then it is a good choice as a site to host this site system role. It is also possible to install this role on a primary site or to install it in multiple locations. Which options you choose depends on the overall configuration of the hierarchy and reporting needs.

2. Select the role in the Add Site System Roles Wizard. Click Next to proceed to the Reporting Service Point page of the wizard, shown in Figure 4.61.

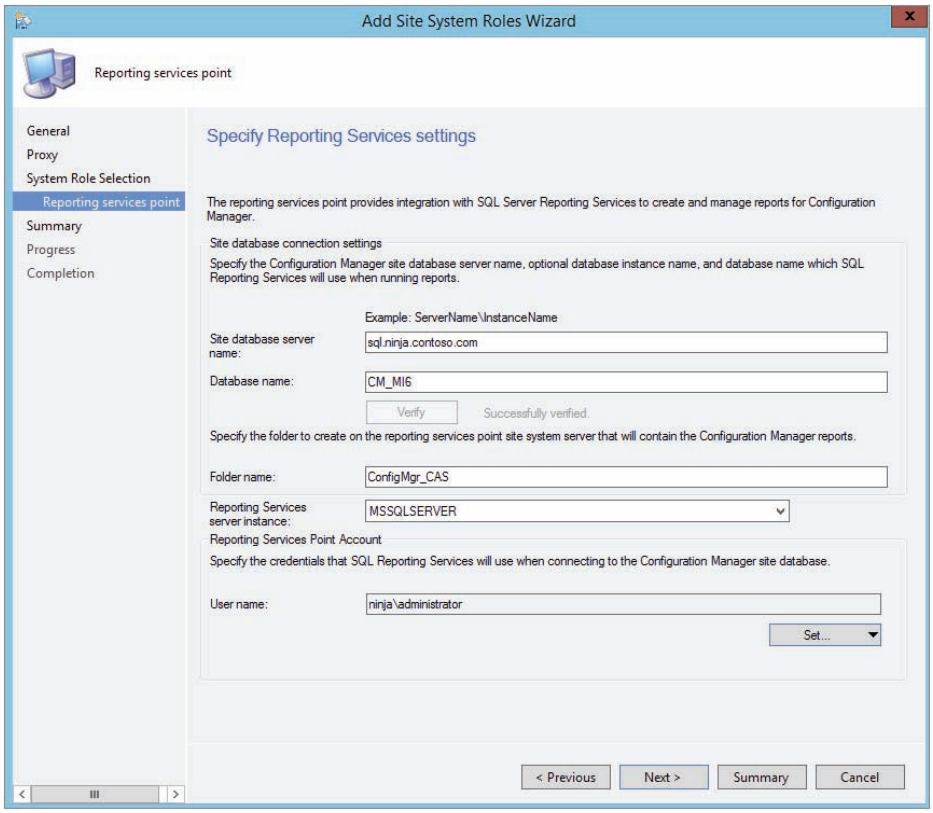


FIGURE 4.61
Add Site System Roles Wizard: Reporting Services Point page

3. On the Reporting Services Point page, provide the server name that is hosting the Configuration Manager database instance and also the database name.

   The server listed here can be the same server hosting the Reporting Services server instance or a remote server.

4. Click Verify to confirm connectivity.

5. Then configure the reporting server component by providing the folder name where the reports will be stored along with the specific SQL Server instance hosting the Reporting Services and the authentication method that will be used for security validation.

   Note that for this section there is no option to specify a server name because it is assumed the site system where the role is being configured is the server hosting the SSRS instance.

6. Once these configurations are complete, click Next.

Software Requirements

The Configuration Manager 2012 R2 Reporting Services point requires that all site servers be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting the Reporting Services Point

The Reporting Services point is the reporting engine for Configuration Manager 2012 R2 and is a key role for most users. Ensuring this role installs and functions correctly is also critical. To provide insight into the proper configuration for this role, the component status is available in the Monitoring node of the console and also by reviewing associated log files.

`srsrpsetup.log` This log tracks the setup status of the reporting point.

`srsrpMSI` This log provides detail status of the reporting point setup process.

`srsrp.log` This log tracks ongoing operational health of the reporting point.

Application Catalog Web Service Point and Application Catalog Website Point

A significant change in Configuration Manager 2012 R2 is its user-centric focus. One component of user-centric focus, and a feature that has been much anticipated, is the ability for users to browse a web page–hosted catalog of published applications available for installation in the environment. These published applications may either be available without restriction to users or configured to require administrative approval prior to installation. Only software deployed to users will appear in the Application Catalog.

Two site system roles work in tandem to provide the Application Catalog service: the Application Catalog web service point and the Application Catalog website point. At first glance, the difference between these two site system roles may not be apparent.

Application Catalog Website Point The Application Catalog website point is the site system providing the software catalog service to users.

Application Catalog Web Service Point The Application Catalog web service point is the site system role that serves as a connection point between the Application Catalog web service point site systems and the Configuration Manager site, providing software information to the website for presentation to users.

About the Example

For the example, the Application Catalog web service point and the Application Catalog website point are presented together. It should not be implied, however, that these site system roles will necessarily be configured on the same server in all cases. While both site system roles are required to facilitate Software Catalog services, they are not required to be configured together.

If the Application Catalog website point and Application Catalog web service point roles have not yet been added, you will need to select them in the Add Site System Roles Wizard, as shown in Figure 4.62.

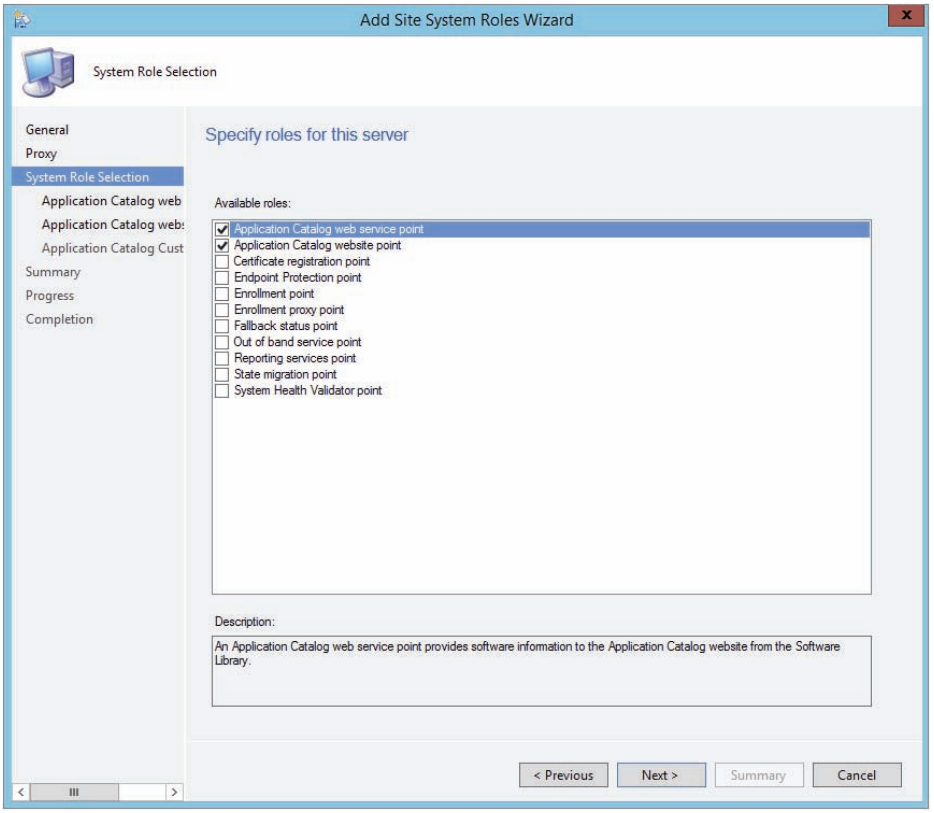


FIGURE 4.62
Add Site System Roles Wizard: Application Catalog website point and Application Catalog web service point selected

1. Choose the site and server where the Application Catalog website point and Application Catalog web service point will be located.

   The exact servers chosen depend on the overall configuration of the hierarchy and mobile management needs.

2. Select the roles in the Add Site System Roles Wizard. Note that the order of the next couple of figures could be different depending on how you choose to install the roles. The net result is the same.

3. Click Next to proceed to the Application Catalog Website Point page of the wizard, as shown in Figure 4.63.

4. On the Application Catalog Website Point page, configure the name for the website to be used.

   Also note the web application name suggested. If the name of the web application is modified on the Application Catalog Web Service Point page, this URL will need to be modified accordingly.

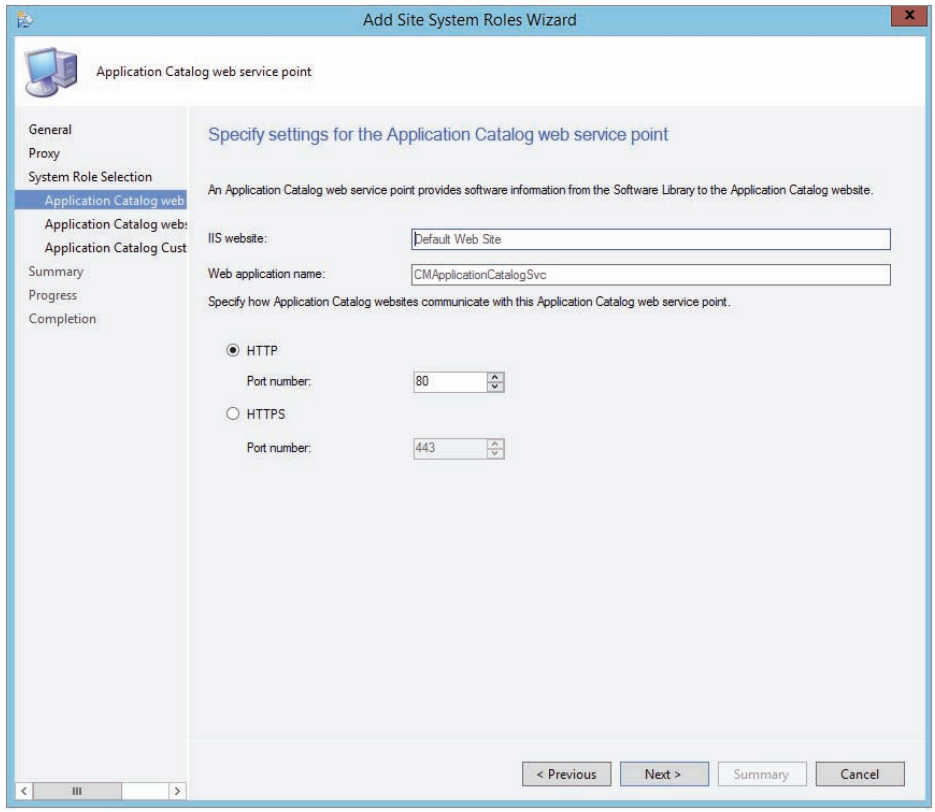


FIGURE 4.63
Add Site System Roles Wizard: Application Catalog Website Point page

5. Also on this page, choose whether the website will support HTTP or HTTPS traffic and, if HTTPS is selected, whether the website will allow only intranet-connected clients or also allow Internet-connected clients.

   Supporting Internet clients requires the use of certificates. In addition, if mobile devices will be supported in the environment, enabling the website to support HTTPS-connected clients is required.

6. Once all configuration is complete, click Next to proceed to the Application Catalog Website Point page, as shown in Figure 4.64.

7. On the Application Catalog Website Point page, configure the web application name for the website to be used and whether the website will use HTTP or HTTPS.

8. Once all configuration is complete, click Next to proceed to the Application Catalog Customizations page. Here administrators are able to provide some minor customization as to the presentation of the catalog (organization name and website theme). Make any modifications desired and click Next to complete the wizard.

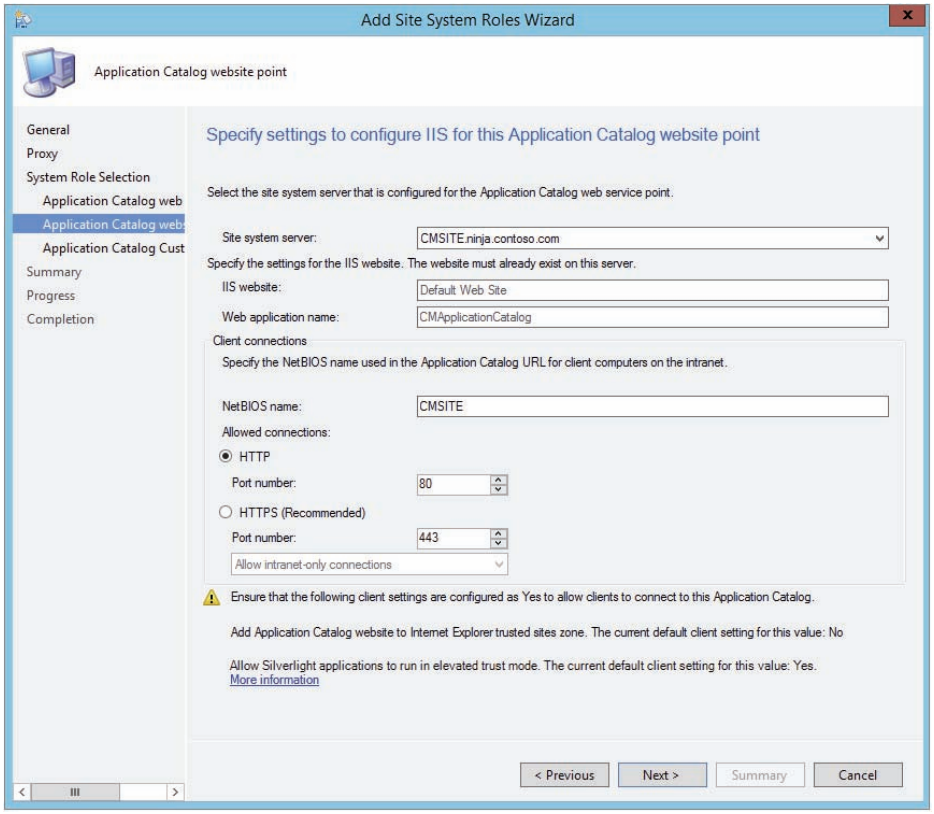


Figure 4.64
Add Site System Roles Wizard: Application Catalog Website Point page

Software Requirements

The Configuration Manager 2012 R2 Application Catalog website point and Application Catalog web service point require the following:

- All site servers must be members of a Windows 2003 or higher Active Directory domain.
- .NET 4.0 must be installed.

Troubleshooting the Application Catalog Website Point and Application Catalog Web Service Point

The Application Catalog roles are key interfaces to enable user self-provisioning of content. Thus, ensuring that these roles are functional is critical. As with all roles, the Monitoring node of the console can provide insight into overall health. In addition, log files are useful to track ongoing operation as well:

`smsawebsvcsetup.log` This log tracks the installation of the application web service.

`smsportwebsetup.log` This log tracks installation of the application web portal.

`awebsvcMSI` This is a detailed MSI log to track installation of the application web service.

`portalwebMSI` This is a detailed MSI log to track installation of the application web portal.

`awebsctrl.log` This log tracks the ongoing operation of the application web service.

`portlctl.log` This log tracks the ongoing operation of the application web portal.

Enrollment Point and Enrollment Proxy Point

Mobile devices have become commonplace in IT environments. With the increase in device number and increasing power and function of these devices, providing management capabilities in the enterprise is becoming more of a focal point for administrators. Configuration Manager 2012 R2 provides two types of management for mobile devices: lite management and depth management.

Lite Management Lite management is provided to any device that is capable of interfacing with Exchange Server through the ActiveSync connector. Such devices include Windows Phone 7 and iPhone and Android devices. Configuration Manager 2012 R2 provides an Exchange Server connector that works with Exchange ActiveSync–connected devices and facilitates settings management, general inventory, and remote wipe capabilities.

Depth Management Depth management is available for legacy Windows phone platforms, such as Windows Mobile 6.1 and 6.5 as well as Nokia Symbian devices, and it allows for a more robust management experience, including the ability to install a native Configuration Manager 2012 client on a device. Depth-managed devices provide all of the features of lite management (though not through Exchange ActiveSync) but also include support for software distribution and over-the-air enrollment. Further, inventory options available for depth-managed clients are more extensive and flexible than those provided through lite management.

Depth-managed devices require a client to be installed, along with certificates to provide access to the various Configuration Manager 2012 R2 systems. Once the client is installed, the device acts similar to a PC, looking up and making use of management points for retrieving policy, sending data such as inventory, and also making use of distribution points for software deployments.

Site Systems and Mobile Devices

Site systems that will interact with mobile devices must be configured to support HTTPS communication. Mobile devices use certificates for authentication and must be able to use these certificates to validate against management points and distribution points (and optionally, Application Catalog servers).

The process of placing the client and certificates on the mobile device, known as enrollment, requires the use of two site system roles: the mobile device enrollment proxy point and the mobile device and AMT enrollment point. These site systems work in tandem to facilitate enrollment, provisioning, and management of mobile devices. At first glance, the difference between these two site system roles may not be apparent.

Enrollment Proxy Point This is the site system role typically placed in the DMZ and is the initial point of communication for devices. It is also the location where mobile devices find and

download the mobile version of the Configuration Manager client. Once the client is installed, and as a part of enrollment, the mobile device enrollment proxy point will communicate with the mobile device and AMT enrollment point, typically located inside the protected network, to retrieve needed certificates and present them to the device being enrolled.

Configuring multiple mobile device enrollment proxy points at a single site to support multiple DMZ configurations is supported.

Enrollment Point This is a site system role typically installed inside the protected network, and it serves as an interface between the mobile device enrollment proxy point and the Enterprise Certificate Authority as certificate requests are presented from mobile devices and generated certificates are sent back to mobile devices.

Certificates are also required for provisioning AMT-capable devices. This site system role also serves as the interface between AMT devices requesting certificates and the Enterprise Certificate Authority.

Tidbits about Site System Roles

It is *not* required that these site system roles exist on the same site system server. If you're using lite management of mobile devices, neither of these site system roles is required.

About the Example

For the example, the mobile device enrollment proxy point and mobile device and AMT enrollment point are presented together. It should not be implied, however, that these site system roles will necessarily be configured on the same server in all cases. While both site system roles are required to facilitate depth management of mobile devices, they are not required to be configured together.

If the enrollment proxy point or the enrollment point roles have not yet been added, you will need to select them in the Add Site System Roles Wizard.

1. Choose the site and server where the enrollment proxy point and enrollment point will be located.

   The exact servers chosen depend on the overall configuration of the hierarchy and mobile management needs.

2. Select the roles in the Add Site System Roles Wizard System Role Selection. Click Next to proceed to the Enrollment Point page of the wizard.

3. On the Enrollment Point page, shown in Figure 4.65, configure the name for the website to be used.

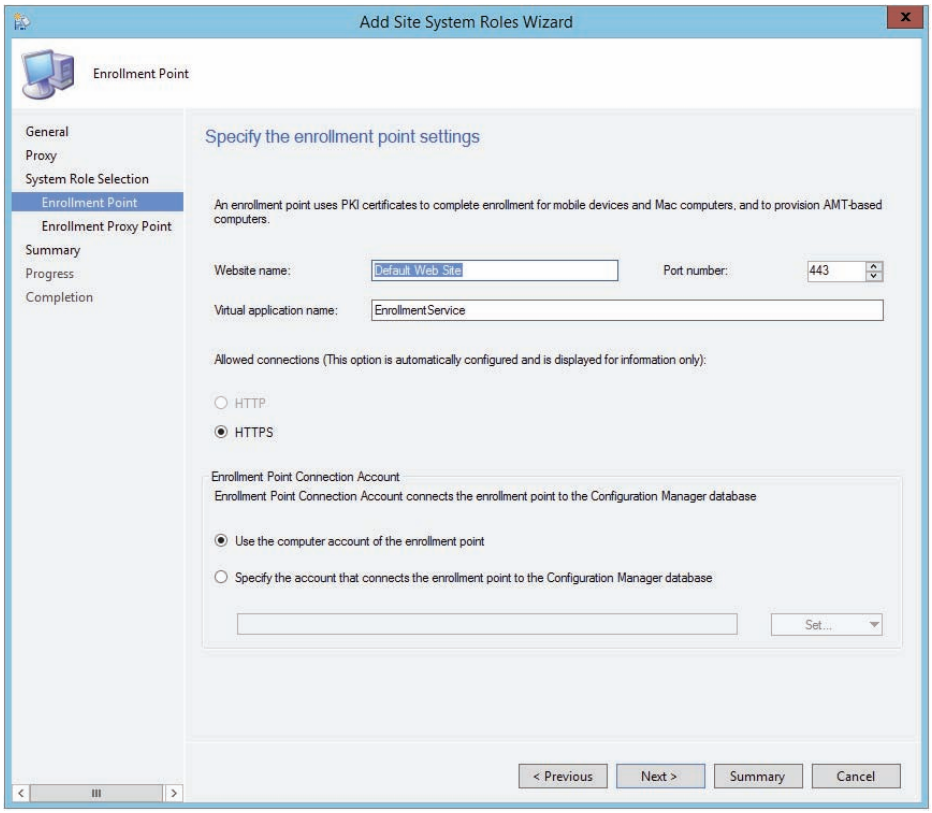


Figure 4.65
Add Site System Roles Wizard: Enrollment Point page

If you make any changes, then the virtual directory name in the URL configured for the mobile device enrollment proxy point must be updated as well. You can also specify which account will be used for database communication. Of the two site system roles, this is the only one that needs to access the database directly.

4. On the Enrollment Proxy Point page, configure the name for the website to be used, as shown in Figure 4.66.

   Note that the website must support SSL communication and that a default URL pointing to the mobile device and AMT enrollment point is already present. This URL is configurable and will need to point to whichever location is chosen to host the mobile device and AMT enrollment point role. Note also that the end of the URL refers to the `EnrollmentService` virtual directory. This is the default name. If a non-default name is chosen for the virtual directory, the URL will need to match.

   Note also that there is a virtual application name listed on the current page that is similar in name. Don't be confused by the similarity; the virtual directory name here is the one used to configure the mobile device enrollment proxy point and is not changeable.

5. Once all configuration is complete, click Next.

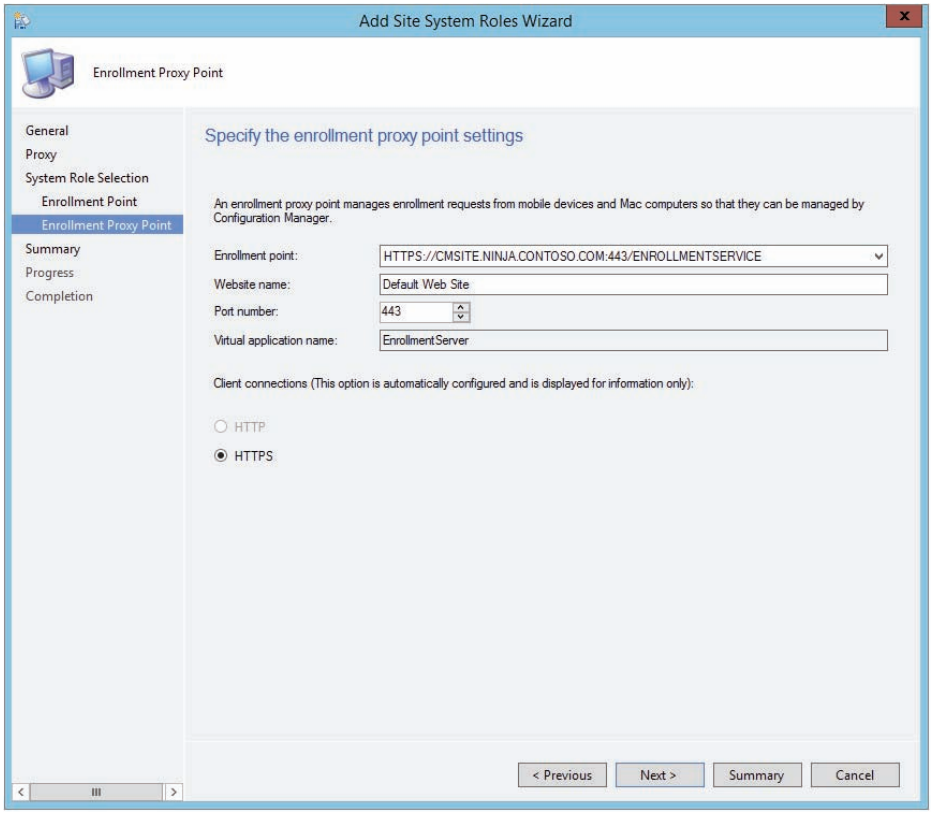


Figure 4.66
Add Site System Roles Wizard: Enrollment Proxy Point page

Software Requirements

The Configuration Manager 2012 R2 mobile device enrollment proxy point and mobile device and AMT enrollment point require that all site servers be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting the Enrollment Proxy Point and Enrollment Point

Enrollment points are the key roles to enable mobile devices and AMT-enabled systems to enter into the ConfigMgr world. To provide insights into the proper configuration of this role, the component status is available in the Monitoring node of the console and also by reviewing the following logs:

`Smsenrollwebsetup.log` This log tracks the installation of the enrollment web proxy point.

`Smsenrollsrvsetup.log` This log tracks the installation of the enrollment web point.

`Enrollwebmsi` This log tracks the installation of the enrollment web proxy point in detail.

Enrollsrvmsi This log tracks the installation of the enrollment web service point in detail.

Enrollweb.log This log tracks the ongoing operation of the enrollment web point.

Enrollsvc.log This log tracks the ongoing operation of the enrollment web proxy point.

Click Next to proceed to the Summary page of the Add Site System Roles Wizard. Review the settings. If all are correct, click Next to proceed with installation and to finish the wizard.

Software Update Point

The software update point role is integral to the software update mechanism and is responsible for synchronizing all patches from Microsoft Update and making them available in the Configuration Manager 2012 R2 interface for deployment. The software update point requires that Windows Software Update Services 3.0 SP2 be installed on the same server where the software update point is being installed and requires that the instance of WSUS be dedicated to interfacing with the software update point and providing service to Configuration Manager. No sharing allowed! Also, administrators should not perform any administrative work on the WSUS server itself. All administrative work should be done through the Configuration Manager console. You will find that the options available in the Configuration Manager console are very similar to what are found in WSUS itself.

If the software update point has not yet been added, you will need to select it in the Add Site System Roles Wizard, as shown in Figure 4.67.

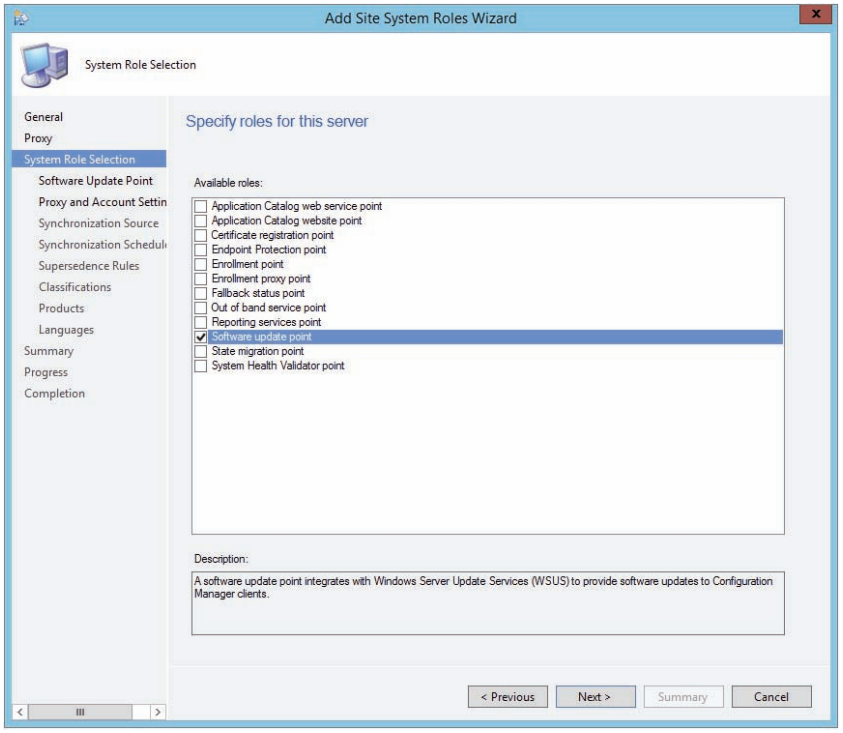


FIGURE 4.67 Add Site System Roles Wizard: System Role Selection page with Software Update Point selected

1. Choose the server where the WSUS component is installed.
2. Select the role in the Add Site System Roles Wizard.
3. Click Next to proceed to the Software Update Point page of the wizard.
4. On the Software Update Point page, configure whether to use ports 80 and 443 for client communications or the customized 8530 and 8531. Determine what kind of client connection type you expect, whether they are intranet-only, Internet-only, or both. Click Next to proceed to the Proxy and Account Settings page of the wizard.
5. A proxy server should be used when synchronizing software updates and also when downloading content with auto deployment rules. Also, choose whether alternate credentials will be used to connect to the WSUS server. If a proxy server is needed, supply the needed information for the proxy server. This is shown in Figure 4.68.
6. Once all configuration is complete, click Next to proceed to the Synchronization Source page of the wizard, shown in Figure 4.69. If software update services will be used in Configuration Manager, at least one software update point is required. Note that a single software update point on properly sized hardware is capable of supporting 100,000 clients in Configuration Manager 2012 R2.

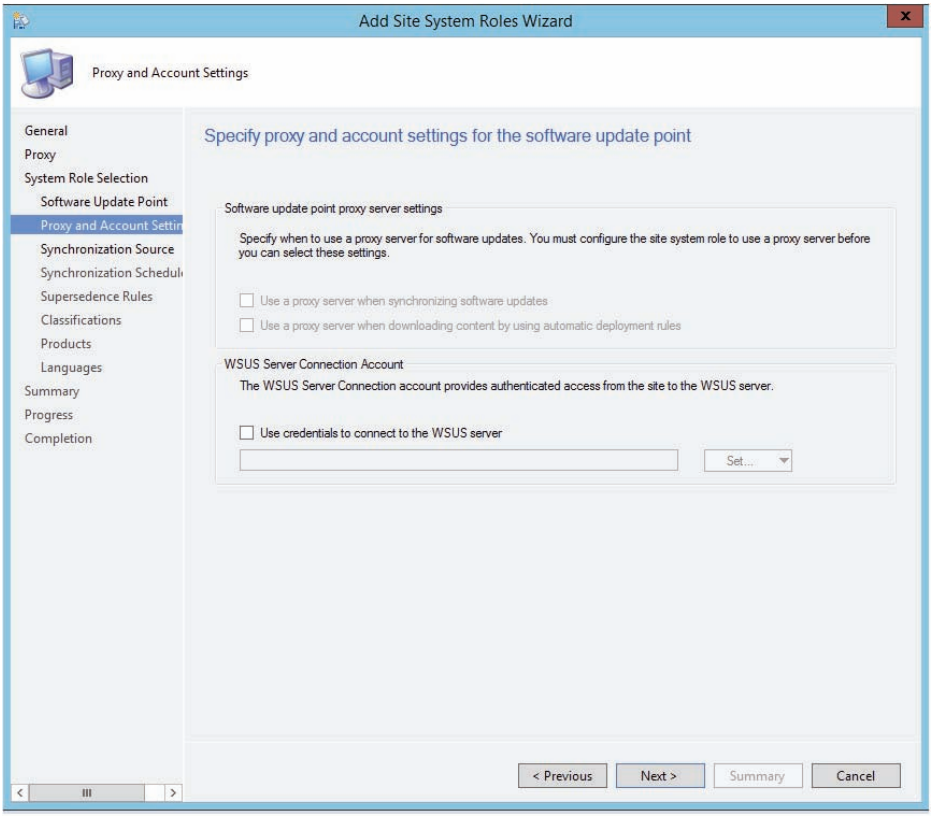


FIGURE 4.68 Add Site System Roles Wizard: Proxy and Account Settings page

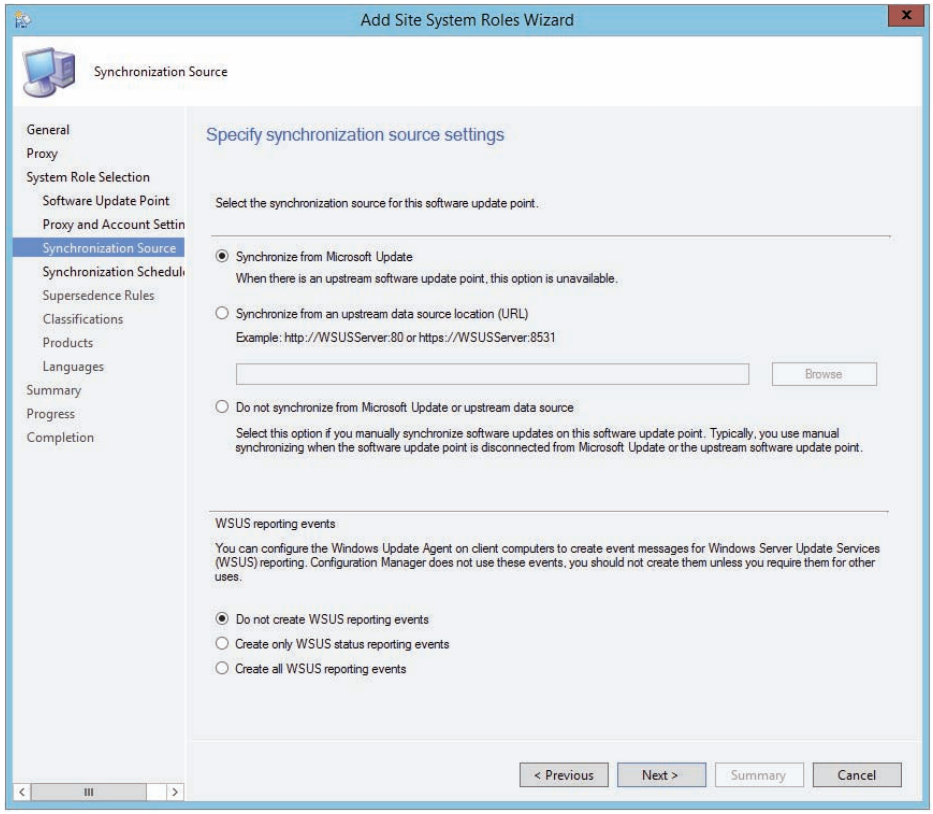


Figure 4.69
Add Site System Roles Wizard: Synchronization Source page

7. On the Synchronization Source page, configure the location that the software update point will use for obtaining update information. Typically this setting will be to synchronize from Microsoft Update from the Internet.

   If this software update point is installed at a child site in a hierarchy, then the option to choose here will be to synchronize from an upstream update point. In this case the CAS would host the top-level software update point and the primary site would synchronize from it.

   If the software update point is on the CAS and the CAS does not have access to the Internet, then it's possible to synchronize manually. If this is the case, choose the option Do Not Synchronize From Microsoft Update Or Upstream Data Source.

8. In the WSUS Reporting Events section, choose whether or not to create any or all WSUS reporting events.

9. Once all configuration is compete, click Next to proceed to the Synchronization Schedule page. Choose whether or not synchronization should proceed on a schedule. It is not required that the software update point be configured to synchronize automatically, but in most environments a recurring schedule is ideal. The schedule is up to you; just

remember that Microsoft publishes new patches the second Tuesday of every month and from time to time will have out-of-band patch releases. If you are using Endpoint Protection in Configuration Manager, it is recommended to perform synchronization no less than daily (or as often as three times per day).

10. If you would like an alert when synchronization fails (a good idea), select that option as well.

11. Once all configuration is complete, click Next to proceed to the Supersedence Rules page shown in Figure 4.70.

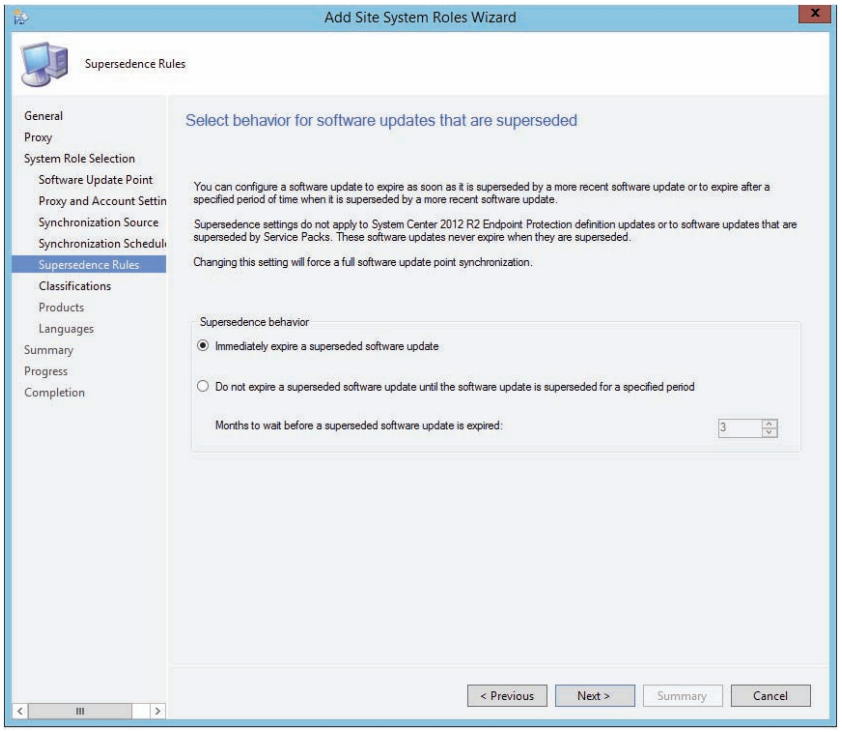


FIGURE 4.70
Add Site System Roles Wizard: Supersedence Rules page

12. On the Supersedence Rules page, choose the behavior that happens when a new update is available and synchronized that replaces an existing update. This option is new to Configuration Manager 2012. The first option, Immediately Expire A Superseded Software Update, is the default, and this was the only option in Configuration Manager 2007. This option caused frustration in many environments—not because an update was superseded, but because the action of superseding also caused the original update to be expired. When an update is expired it can no longer be deployed. While it is a good idea to stop deploying a superseded update when it has been replaced, the truth is that testing cycles in many environments do not easily allow for this kind of rapid change. For that reason, the second choice (Months To Wait Before A Superseded Software Update

Is Expired) was made available in Configuration Manager 2012 R2. Note that the superseded update is still superseded; it just isn't expired and can still be deployed.

13. Once all configuration is complete, click Next to proceed to the Classifications page shown in Figure 4.71.

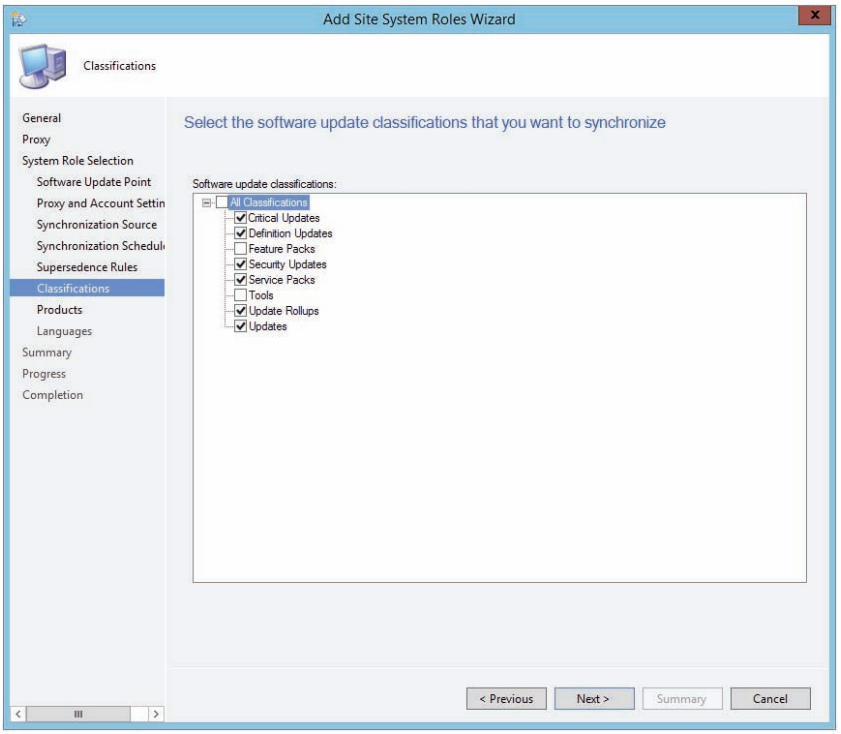


FIGURE 4.71
Add Site System Roles Wizard: Classifications page

14. On the Classifications page, choose the classifications of updates that should be retrieved from Microsoft Update and made available in Configuration Manager 2012 R2 for deployment.

15. Once all configuration is complete, click Next to proceed to the Products page shown in Figure 4.72.

16. On the Products page, choose the products or product families that should be included when retrieving updates from the categories just configured. The expanded list is shown in the figure.

17. Once all configuration is complete, click Next to proceed to the Languages page. Here, choose all languages that are in use in your environment. This will ensure the appropriate language-specific patches are included during synchronization as well.

18. Once all configuration is complete, click Next and proceed through the remaining wizard pages to complete the configuration.

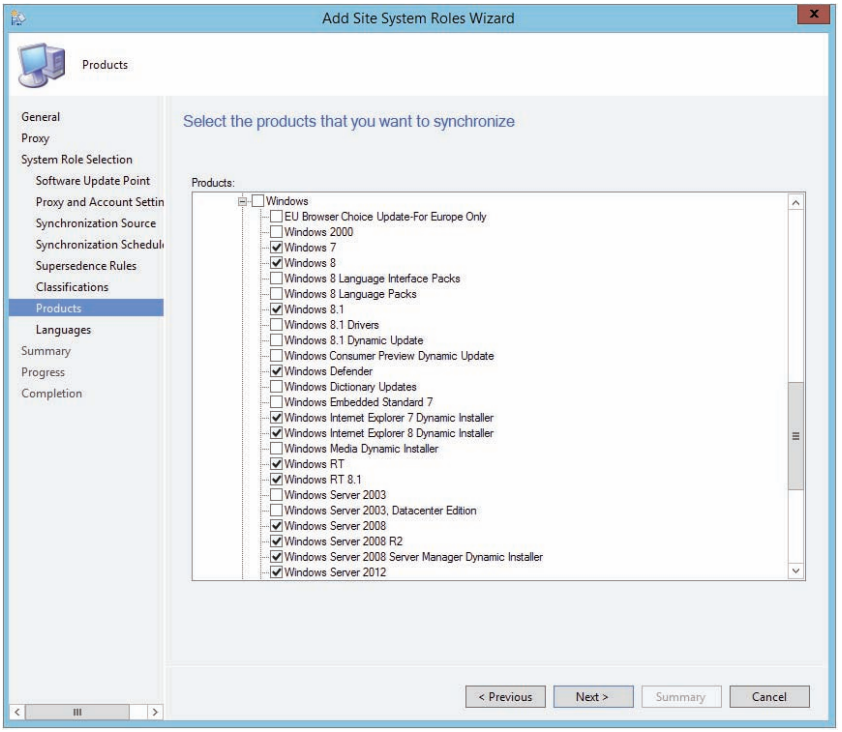


Figure 4.72
Add Site System Roles Wizard: Products page

Software Requirements

The Configuration Manager 2012 R2 software update point requires that all site servers must be members of a Windows 2003 or higher Active Directory domain. In addition, the software update point requires WSUS 3.0 SP2 and Internet Information Services to be installed. It's also a good idea to install WSUS 3.0 SP2 hotfixes KB2720211 and KB2734608 (in that order) to ensure stability and performance in WSUS and your software update point.

Troubleshooting the Software Update Point

The proper installation of the software update point is key to delivering updates through Configuration Manager 2012 R2 in your environment. To provide insights into the proper configuration of this role, the component status is available in the Monitoring node of the console and also by reviewing the following logs:

`Supsetup.log` This log tracks the installation of the software update point.

`WCM.log` This log tracks connections to the WSUS server for subscribed update categories, languages, and classifications.

`WSUSCtrl.log` This log tracks connectivity to the database and the general health of WSUS for the site.

`WSYNCMGR.log` This log records all synchronization operations for the site.

Endpoint Protection Point

If you will be using Configuration Manager 2012 R2 for Endpoint Protection services, then you must install the Endpoint Protection point role. This role is available only at the CAS and requires that separate licensing be in place. Installing this role is very easy and simply enables the use of Endpoint Protection in the hierarchy.

If the Endpoint Protection point has not yet been added, you will need to select it in the Add Site System Roles Wizard:

1. Choose the server where the Endpoint Protection point will be located.
2. Select the role in the Add Site System Roles Wizard. Note that when you attempt to place a check mark in the role, you will see a popup notifying you of default configurations that will be set.
3. On the Endpoint Protection page, accept the license agreement.
4. Once all configuration is complete, click Next to proceed to the Microsoft Active Protection Service page, shown in Figure 4.73.
5. On the Microsoft Active Protection Service page, read the description of the Active Protection Service membership, and choose what type of membership you would like, if any.
6. Once all configuration is complete, click Next through the wizard to complete installation.

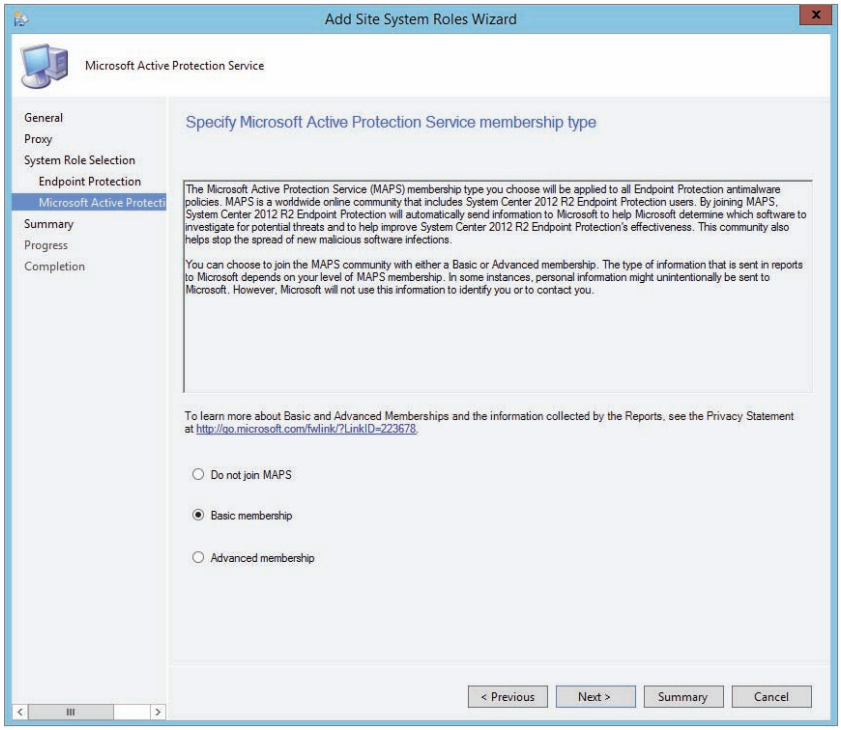


FIGURE 4.73 Add Site System Roles Wizard: Microsoft Active Protection Service page

Software Requirements

The Configuration Manager 2012 R2 Endpoint Protection point requires that all site servers be members of a Windows 2003 or higher Active Directory domain.

Troubleshooting the Endpoint Protection Point

The proper installation of the Endpoint Protection point is key to managing malware and firewall settings through Configuration Manager 2012 R2 in your environment. To provide insights into the proper configuration of this role, the component status is available in the Monitoring node of the console and also by reviewing the following logs:

`EPsetup.log` This log tracks the installation of the Endpoint Protection point.

`EPCtrlmgr.log` This log details the synchronization of malware threat information from the Endpoint Protection role server to the Configuration Manager 2012 R2 database.

`EPMgr.log` This log monitors the status of the Endpoint Protection site system role.

Asset Intelligence Synchronization Point

If you will be using Configuration Manager 2012 R2 for Asset Intelligence information, then you will likely want to install the Asset Intelligence synchronization point role. This role is available only at the CAS and is not required but is beneficial. Installing this role enables synchronizing of catalog updates from the Internet and also allows you to upload custom catalog requests and categorization information to Microsoft.

If the Asset Intelligence synchronization point has not yet been added, you will need to select it in the Add Site System Roles Wizard.

1. Choose the server where the Asset Intelligence synchronization point will be located.
2. Select the role in the Add Site System Roles Wizard.
3. On the Asset Intelligence Synchronization Point Settings page, select whether to use this system as the active system and, if you have a certificate, the UNC path where it can be found. Note that the use of a certificate is not required. This is shown in Figure 4.74.
4. Once all configuration is complete, click Next to proceed to the Specify The Synchronization Schedule page. Here, configure the schedule you would like to use for synchronizing the catalog and also sending your update requests for the catalog to Microsoft. Typically, the default schedule is appropriate.
5. Once all configuration is complete, click Next through the wizard to complete installation.

Software Requirements

The Configuration Manager 2012 R2 Asset Intelligence synchronization point requires that all site servers be members of a Windows 2003 or higher Active Directory domain.

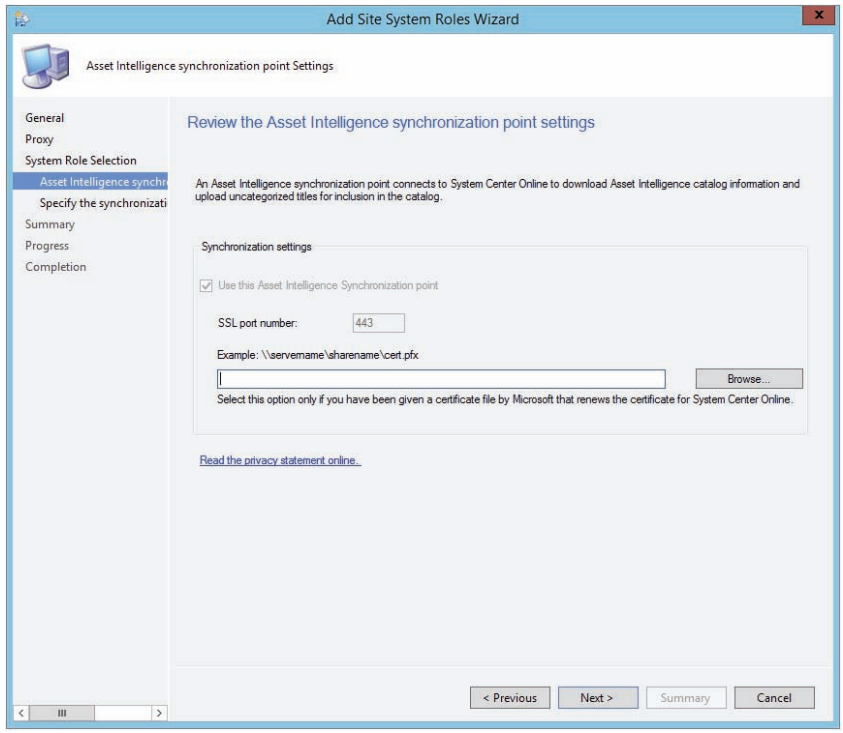


FIGURE 4.74
Add Site System Roles Wizard: Asset Intelligence Synchronization Point Settings page

TROUBLESHOOTING THE ASSET INTELLIGENCE SYNCHRONIZATION POINT

The proper installation of the Asset Intelligence synchronization point is key to keeping your Asset Intelligence catalog up to date for use in Configuration Manager 2012 R2. This is also critical to communicate your requested updates to the catalog to Microsoft. To provide insights into the proper configuration of this role, the component status is available in the Monitoring node of the console and also by reviewing the following logs:

`AIUSsetup.log` This log tracks the installation of the Asset Intelligence synchronization point.

`AIUSMSI.log` This log tracks the specific MSI installation process detail for the Asset Intelligence synchronization point.

`AIUpdateSvc.log` This log tracks the ongoing operation of the Asset Intelligence synchronization point.

The Bottom Line

Understand Configuration Manager 2012 R2 sites and the new approach to hierarchy design. Configuration Manager 2012 R2 has three types of sites: the Central Administration Site, which is new, and the primary and secondary sites, which are familiar. Although two of the three site types are familiar, their use and approach to hierarchy design—or whether a hierarchy is needed at all—are quite different now.

> **Master It** Describe the purpose of each site type and map each to specific management needs.

Construct a Configuration Manager 2012 R2 hierarchy. The site hierarchy in Configuration Manager 2012 R2 consists of the site types just described. The approach to design is very different from the previous version, with the number of primary sites being limited to a single tier. The chapter walked through configuring a hierarchy with all three site types.

> **Master It** Describe a Configuration Manager 2012 R2 site hierarchy. Detail components needed for site-to-site communication and security settings.

Determine when to expand a hierarchy and when to simply add a site system role for additional service. A major design goal of Configuration Manager 2012 R2 is simplified hierarchy design. Administrators familiar with previous versions of Configuration Manager may be tempted to retain old hierarchy approaches when designing Configuration Manager 2012 R2. Taking such an approach will often lead to inefficient designs and additional server cost and in some cases simply won't work.

> **Master It** Understand the changes in sites and site components that lend themselves to hierarchy simplification and enable parity management with fewer site servers.

Deploy and configure the various site system roles available per site. There are many roles available to enable management at a site. Understanding each role and the service it delivers is critical to getting the most out of an investment in Configuration Manager 2012 R2.

> **Master It** Review critical system roles and understand the services that are enabled through each.



Chapter 5

Cloud Integration

Ever since the release of Configuration Manager 2012 Service Pack 1, you can use Windows Azure cloud services to host cloud-based distribution points. Cloud-based distribution points allow Configuration Manager administrators to provide content to Internet-facing clients quickly and easily, without having to deal with the complexity of setting up Configuration Manager site systems in a perimeter network. Just like on-premises distribution points, cloud-based distribution points can be managed individually, or they can be members of distribution point groups.

Cloud-based distribution points have many benefits; for instance, they can be used for fallback content location. In addition, the provisioning of content on cloud-based distribution points is a secure process; Configuration Manager 2012 encrypts the content that is targeted to cloud-based distribution points before the content is sent to Windows Azure. Another benefit of cloud-based distribution points on Windows Azure is that the service can scale to meet changing demands for content requests, without having to deploy additional distribution points.

Windows Azure and cloud-based distribution points in Configuration Manager 2012 provide you with a lot of flexibility. You can extend and integrate your private cloud Configuration Manager infrastructure with the public cloud in a matter of hours—maybe in a couple of days in most cases. How long will it take you to requisition hardware or a virtual machine, stage the OS and applications, and then work with your network and security teams to set up that server in a perimeter network? In most environments that project will take months to complete.

Another benefit of cloud integration is that you can scale on the fly your cloud-based distribution points, based on your Internet-connected users' demand. You can control the costs that are associated with data transfers to and from a cloud-based distribution point; Configuration Manager includes options to control and monitor data access. You can also control and monitor the amount of content that you copy to the cloud service, and you can configure Configuration Manager to alert you when thresholds for client downloads meet or exceed monthly limits. Use the alerts in Configuration Manager to proactively manage data charges when you use cloud-based distribution points.

You might be wondering where you can use a cloud-based distribution point. My experience supporting Configuration Manager for some of the Fortune 500 companies in the United States tells me that most enterprises could benefit from cloud-based distribution points. One retailer I know could prevent all his remote stores' computers from coming across the WAN to get content from their corporate network. An oil company I know could have the computers on drilling rigs located in the middle of the ocean pull the content they need from the cloud. An insurance company I know could probably eliminate over 20,000 secondary sites/distribution

points that they have in every remote office—yes, the offices you see in your neighborhood. I could go on. With the trend of more and more employers allowing for telecommuting, I expect to see a lot of you using cloud-based distribution points in the near future.

Cloud-based distribution points have some limitations. They cannot host software updates packages and cannot be used for PXE or multicast operating system deployments. Cloud-based distribution points cannot be configured as pull distribution points. They do not support prestaged content, and the primary site that manages the distribution point encrypts and copies the content to the distribution point on Windows Azure. The encryption key used to encrypt the content is different for each package. Because of that, cloud-based distribution points do not support Single Instance Storage. In addition, cloud-based distribution points do not support packages configured to run from the distribution point; all content must be downloaded to the client cache and executed locally. Because of that limitation, clients are not offered a cloud-based distribution point as a content location when a task sequence uses the Download Content Locally When Needed By Running Task Sequence option. On the other hand, if the task sequence is configured with the Download All Content Locally Before Starting Task Sequence option, a cloud-based distribution point will be offered as a valid content location. Another limitation is that cloud-based distribution points do not support streaming of App-V applications.

In this chapter, you will learn to

- Test cloud distribution points before going into production
- Control cloud distribution points usage costs
- Simplify your hierarchy

Windows Azure Integration

Windows Azure is Microsoft's cloud platform. It allows you to quickly build, deploy, and manage applications across a global network of Microsoft-managed datacenters. Windows Azure is an open and flexible platform that allows you to integrate your existing IT environment with public cloud applications. Support for cloud-based distribution points in Configuration Manager 2012 is a good example of how Windows Azure allows you to integrate and expand your private cloud environment with public cloud applications. To be able to use Configuration Manager 2012 integration with Windows Azure and deploy a cloud-based distribution point, you must meet some prerequisites:

- You must have a Windows Azure service subscription.
- You must have a self-signed or public key infrastructure (PKI) management certificate. This can be created with Visual Studio Express.
- You must set the client setting Allow Access To Cloud Distribution Points under Cloud Services to Yes.
- You must have a PKI service certificate for the clients to use to connect to cloud-based distribution points. You will need either a Microsoft or a third-party PKI infrastructure and a way to issue the certificate.
- Clients must have Internet access to use the cloud-based distribution point.
- Clients must be able to resolve the name of the cloud service, so a Domain Name System (DNS) record is required in your DNS namespace.

Management Certificate for Site Server to Distribution Point Communication

The communication between Configuration Manager 2012 and cloud-based distribution points is secured and encrypted. Microsoft wants to make sure your content is well protected, so every package is encrypted with a different encryption key before it gets copied to the cloud-based distribution points. To make this process secure, you will need a couple of certificates. In this section, you will find information about the certificate requirements and also about other requirements for the clients to be able to communicate with cloud-based distribution points.

- The management certificate establishes trust between Windows Azure and Configuration Manager. This authentication enables Configuration Manager to call on the Windows Azure API when you perform tasks such as deploying content to the cloud-based distribution point. Windows Azure subscribers can create their own management certificates, which can be either a self-signed certificate or a certificate that is issued by a certification authority (CA). This certificate will have to be exported as a `.pfx` file and a `.cer` file.
- The `.cer` file of the management certificate is the one that has to be uploaded to Windows Azure. If your company is already using Windows Azure, there is a very good chance that a management certificate was already created and uploaded there. In that case you will only need to get the `.pfx` file and its password. If that is not the case, the certificate will have to be uploaded to the Windows Azure portal. We will cover that in the next section. The `.cer` file contains the public key for the management certificate. You must upload this certificate to Windows Azure before you create a cloud-based distribution point in the Configuration Manager Administration console.
- The `.pfx` file of the management certificate is provided to Configuration Manager when you create the cloud-based distribution point. The `.pfx` file contains the private key for the management certificate. Configuration Manager stores this certificate in the site database. Because the `.pfx` file contains the private key, you will be prompted for the certificate password.
- The service certificate is the other certificate you are going to need as a `.pfx` file. This certificate is provided to Configuration Manager when creating the cloud-based distribution point. The service certificate establishes trust between the Configuration Manager clients and the cloud-based distribution point. The service certificate also secures the data that clients download from the cloud-based distribution point by using Secure Socket Layer (SSL) over HTTPS.
- Clients must be able to access the Internet to be able to use cloud-based distribution points. They also need to be able to resolve the name of the cloud-based distribution point. This requires a DNS alias and a CNAME record in your DNS namespace.

Creating a Cloud Distribution Point

This section covers creating the certificates, requesting and exporting the certificates, uploading the management certificate to Windows Azure, and finally creating the cloud-based distribution point. If you are an MSDN subscriber or have access via a corporate subscription, you have access to a limited Windows Azure subscription that will allow you to test

cloud-based distribution points. You could also sign up for a free Windows Azure trial to test cloud-based distribution points.

We are going to show you how to use Visual Studio Express 2013 to create the management certificate. Since it would be impossible to cover every public key infrastructure (PKI) service in this book, we are going to use Microsoft's PKI services to create the service certificate. If you are using a different PKI service, please refer to the "PKI Certificate Requirements for Configuration Manager" TechNet article available at `http://technet.microsoft.com/en-us/library/gg699362`.

Creating and Exporting the Management Certificate

To create the management certificate, you will use Visual Studio Express 2013. You can get it free from `www.microsoft.com/visualstudio/eng/downloads`. You don't need to install Visual Studio on your Configuration Manager server. You can install Visual Studio on your workstation or on any other computer since you are going to export the certificate after its creation.

1. Install Visual Studio Express 2013. Go to the Visual Studio Tools and open as administrator Developer Command Prompt for VS2013. In the command prompt window run the following command, as shown in Figure 5.1:

   ```
   makecert -sky exchange -r -n "CN=Windows Azure Management Certificate"
   -pe -a sha1 -len 2048 -ss My "Windows Azure Management Certificate.cer"
   ```

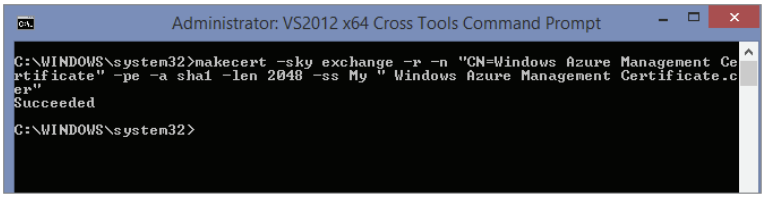


FIGURE 5.1 Creating the Windows Azure Management Certificate

2. Open the MMC, add the Certificates snap-in, and then select My User Account. Click Finish and then click OK.
3. Under Certificates expand Personal, and then expand Certificates.
4. Right-click the Windows Azure Management Certificate, select All Tasks, and then select Export.
5. Click Next, select No, Do Not Export The Private Key, and then click Next. See Figure 5.2.
6. Make sure DER Encoded Binary X.509 (.CER) is selected, and then click Next, as shown in Figure 5.3.

FIGURE 5.2
Exporting the private key

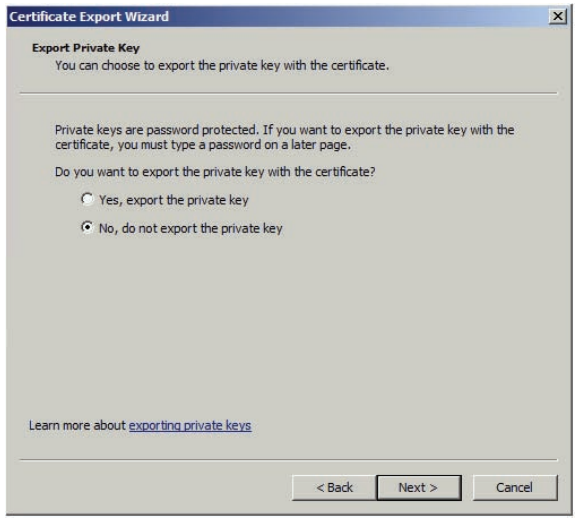
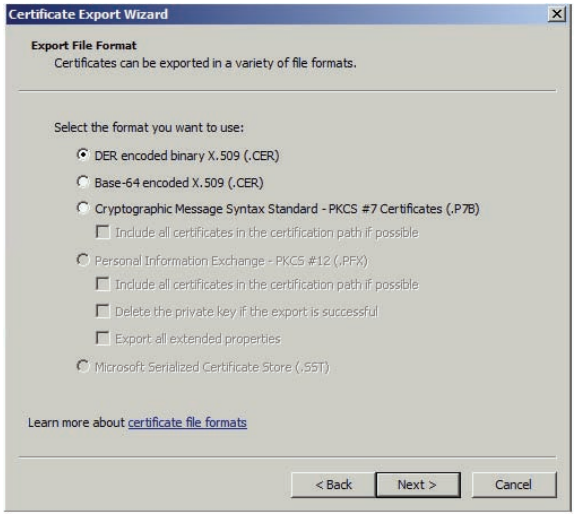


FIGURE 5.3
DER encoded binary



7. Specify a name for the certificate such as Windows Azure Management Certificate, and then click Next. See Figure 5.4.
8. Click Next, and then click Finish.
9. Click OK on the Export Was Successful dialog box.

   Note that if you do not specify a patch for the certificate, the `.cer` file will be saved under `…\Windows\System32`.

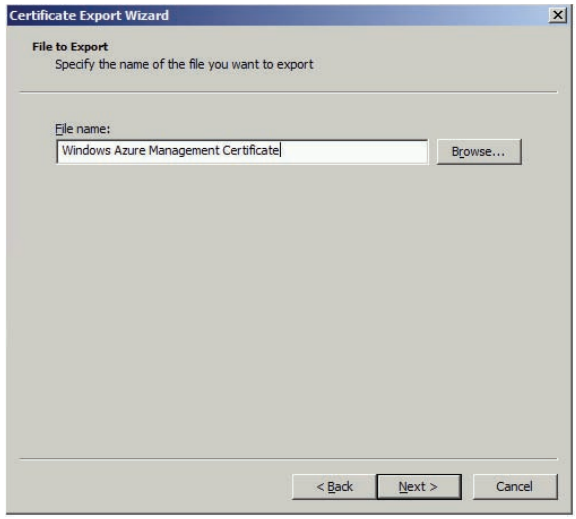


FIGURE 5.4 Name the certificate

10. You need to export the management certificate one more time but this time as a `.pfx` file. Under Certificates expand Personal, and then expand Certificates.
11. Right-click Windows Azure Management Certificate, select All Tasks, and then select Export.
12. Select Yes, Export The Private Key and then click Next, as shown in Figure 5.5.
13. Click Next, provide a password for the certificate, and then click Next again.

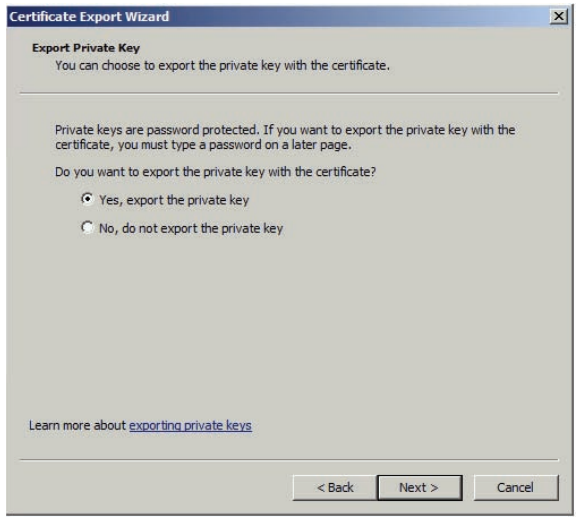


FIGURE 5.5 Exporting the private key

14. Provide a name for the certificate such as Windows Azure Management Certificate, and then click Next. Click Finish. Click OK to dismiss the Certificate Export Wizard successful completion message. Again, if you do not specify a patch for the certificate, the `.pfx` file will be saved under …`\Windows\System32`.

15. Now is a good time to copy the management certificates' `.cer` and `.pfx` files to a safe location.

Creating the Service Certificate Template

To create the service certificate, you are going to use Microsoft's PKI services. In most enterprises, we don't expect the Configuration Manager administrators to have access to the PKI services. PKI is something that is usually managed by another team. The following steps and the "PKI Certificate Requirements for Configuration Manager" TechNet article mentioned earlier can be used as references by the PKI team. We will be creating the service certificate on the Enterprise CA, but the PKI services configuration in your environment will dictate where you need to create this certificate.

1. Before you create the cloud-based distribution point service certificate, create a security group named ConfigMgr Site Servers and add all the Configuration Manager SP1 primary site servers that will be managing cloud-based distribution points.

2. Open the Certification Authority console on the Enterprise CA, right-click Certificate Templates, and then click Manage to load the Certificate Templates management console.

3. Right-click the Web Server entry in the column Template Display Name, and then click Duplicate Template, as shown on Figure 5.6.

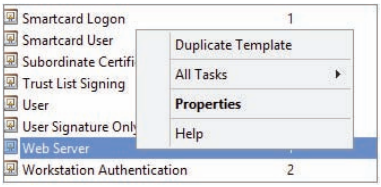


Figure 5.6
Select Duplicate Template.

4. In the Duplicate Template dialog box, ensure that Windows 2003 Server is selected for compatibility.

5. In the Properties Of New Template dialog box, on the General tab, enter a template name to generate the web server certificate for cloud-based distribution points, such as ConfigMgr Cloud-based Distribution Point Certificate.

6. On the Request Handling tab, select Allow Private Key To Be Exported.

7. On the Cryptography tab, change Minimum Key Size to 2048.

8. On the Security tab, remove the Enroll permission from the Enterprise Admins and Domain Admins security groups.

9. Click Add, enter **ConfigMgr Site Servers** in the text box, and then click OK.
10. Check the Enroll permission for this group, and do not uncheck the Read permission.
11. Under the Subject Name tab make sure Supply In The Request is selected.
12. Click OK and close the Certificate Templates console.
13. In the Certification Authority console, right-click Certificate Templates, click New, and then click Certificate Template To Issue.
14. In the Enable Certificate Templates dialog box, select the new template that you have just created, ConfigMgr Cloud-based Distribution Point Certificate, and then click OK.
15. Close the Certification Authority console.

Requesting and Exporting the Service Certificate

In the previous section, you created the service certificate template on the Enterprise CA. In this section, you will request and export the service certificate. Perform the following steps on the primary site that is going to be managing cloud-based distribution points:

1. On the Configuration Manager SP1 site that is going to manage a cloud-based distribution point, open the MMC, add the Certificates snap-in and the Computer account, and then select Local Computer. Click Finish and then click OK.
2. Expand Personal and then right-click Certificates. Select All Tasks and then Request New Certificate, as shown in Figure 5.7.

FIGURE 5.7
Request New Certificate



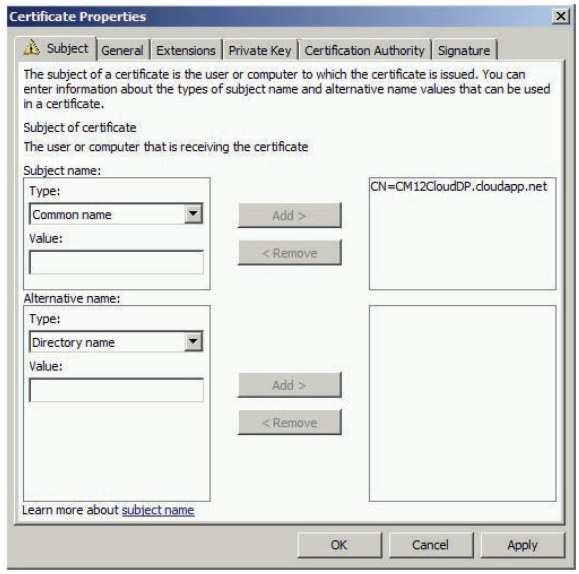
3. Accept the default options on the Certificate Enrollment Wizard until a list of available certificates is displayed.
4. Select the ConfigMgr Cloud-based Distribution Point certificate, and then click More Information Is Required To Enroll For This Certificate. Click Here To Configure Settings. That would be the line with the exclamation mark in a yellow triangle, as shown in Figure 5.8.
5. In the Certificate Properties window's Subject tab, under Subject Name, select Common Name. In the Value field for Common Name, type **CM2012R2CloudDP.cloudapp.net** and then click Add. See Figure 5.9.

   Note that the common name in the certificate subject box must be unique in your domain and not match any domain-joined device.

FIGURE 5.8
More information



FIGURE 5.9
Certificate Properties dialog



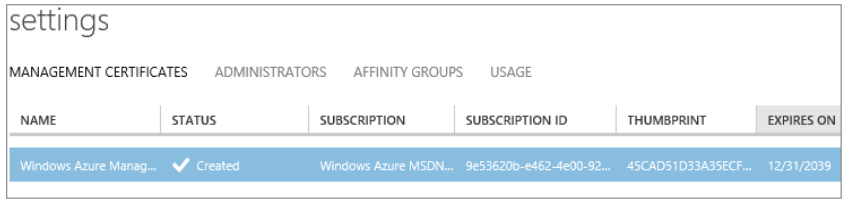
6. Click OK, click Enroll, and then click Finish.
7. Find the service certificate in the Certificates console, right-click it, select All Tasks, and then click Export.
8. Follow the Certificate Export Wizard and select Yes, Export The Private Key.
9. Click Next, provide a password for the certificate, and then click Next again.
10. Provide a name for the certificate like ConfigMgr Cloud-based Distribution Point Service Certificate, click Save, and then click Next.
11. Click Finish. Again, if you do not specify a patch for the certificate, the `.pfx` file will be saved under …\`Windows\System32`. Save the service certificate `.pfx` file to a safe location.

Uploading the Management Certificate to Windows Azure

If your company has a Windows Azure subscription and they have already created a management certificate for Windows Azure, there is no need to upload another certificate. You can use the existing certificate as long as you can get its `.pfx` file and its password. In that case you can skip this section. If there is no Windows Azure management certificate already in place, use the following steps to upload the management certificate to Windows Azure:

1. Open and log on to the Windows Azure Management Portal (`http://management.windowsazure.com`).
2. Click Settings, and then click Management Certificates.
3. Click Upload A Management Certificate and browse to the `.cer` certificate that you create earlier. Click the check mark to upload the certificate. After the certificate is uploaded successfully, you should be able to see it in the Windows Azure Management Portal, as shown in Figure 5.10.

FIGURE 5.10 Management Certificates



Creating the Cloud Distribution Point

Now that you have taken care of all the prerequisites, you can go to the Configuration Manager Administration console to create the cloud-based distribution point.

1. Open the Configuration Manager Administration console.
2. Under Administration, expand Cloud Services, and then click Cloud Distribution Point.
3. Click Create Cloud Distribution Point. When the Create Cloud Distribution Point Wizard opens, enter your Windows Azure Subscription ID and browse to the `.pfx` management certificate you exported after creating it in Visual Studio. If your company already had a management certificate created for Windows Azure, select that `.pfx` file instead. Your Windows Azure Subscription ID is not the email address you used to open your Windows Azure subscription; it is actually a long string of numbers that you can get under the Windows Azure Cloud Services Dashboard.
4. Enter the password for the `.pfx` management certificate, and then click Next.
5. The service name is created automatically. Enter a description for the distribution point, select a region, and make sure the primary site managing the cloud-based distribution point is selected. Under Specify A Server PKI For This Cloud Service, browse to the `.pfx` file for the Cloud-Based Distribution Point Service Certificate (enrolled from your certificate authority) and enter its password. The Service FQDN field will be populated automatically with the service name you specified in the certificate. See Figure 5.11.
6. Configure alerts for the cloud-based distribution point as you want, and then click Next. See Figure 5.12 for the default values.

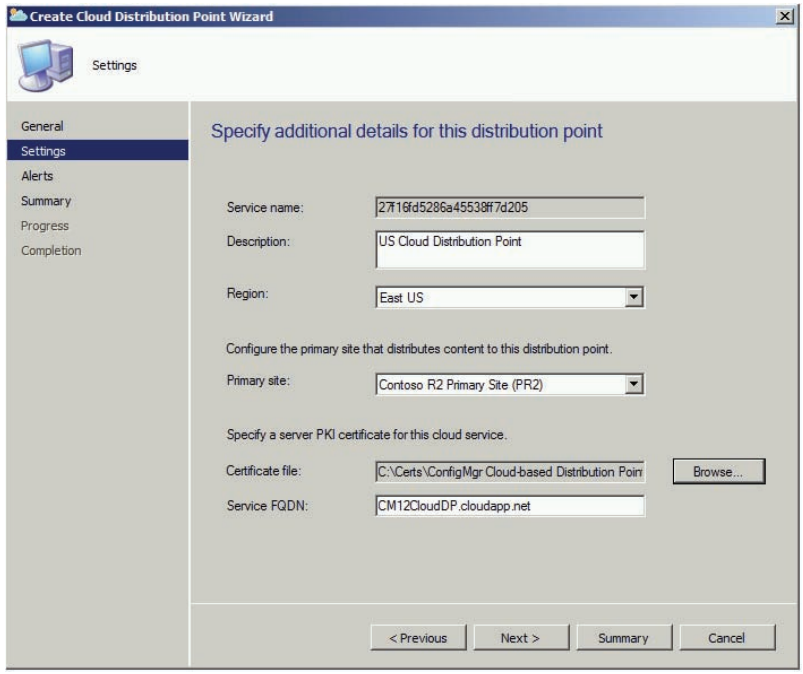


FIGURE 5.11
Creating a cloud distribution point

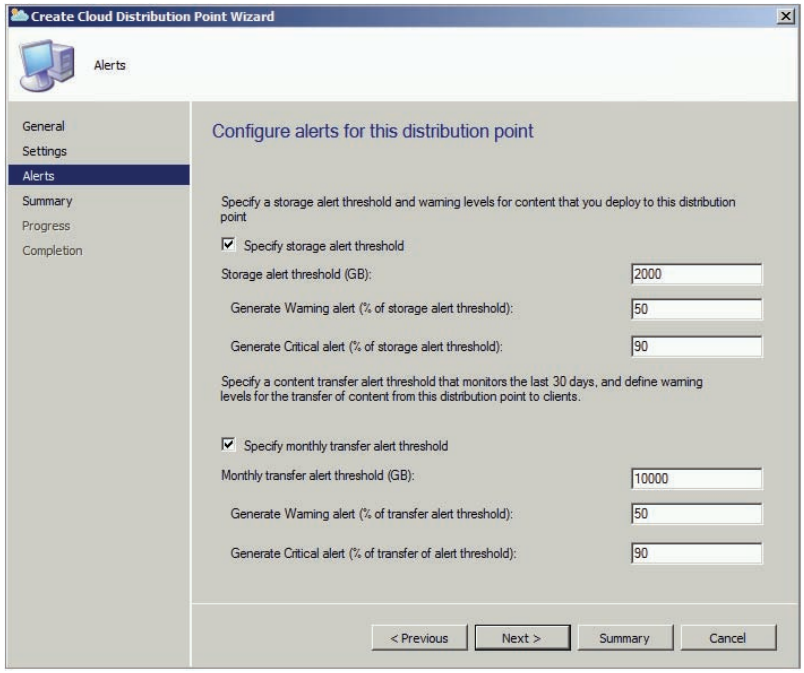


FIGURE 5.12
Configuring alerts

7. Click Next one more time on the Summary page, and then click Close after the cloud-based distribution point is created.

8. You can use the Configuration Manager Trace Log tool to open the Cloud Services Manager log file (`CloudMgr.log`) to monitor the cloud-based distribution point creation process. You will see entries like these in the log:

```
Skipping safe exception Microsoft.Windows Azure.StorageClient
.StorageServerException. Will check again in 10 seconds.

Waiting for check if container exists. Will check again in 10 seconds.
```

   After five minutes you will see the following error in the log:

```
ERROR: Timed out after 00:05:00 minutes waiting for check if container exists.
```

   Do not worry about the timeout error; the provisioning process will continue behind the scenes on Windows Azure. You can go to the Windows Azure portal under Cloud Services and also under Storage and check that a new cloud service and storage are getting created with the service name generated by the Create Cloud Distribution Point Wizard. Later, in the Cloud Services Manager log, you will see that Configuration Manager started uploading `contentwebrole.cspkg` to Windows Azure.

9. You can also use the Configuration Manager console to make sure the cloud-based distribution point is provisioned before you start copying content to it. Under Administration, expand Cloud Services, and then click Cloud Distribution Points. Make sure that the Status field for the cloud distribution point shows Ready. The Status Description should be Provisioning Completed.

10. Test deploying content to the cloud-based distribution point. Choose an application in the Configuration Manager console and distribute it to the newly created cloud-based distribution point. Choose Monitoring ➢ Content Status in the Configuration Manager Administration console to make sure content got copied to the cloud-based distribution point.

11. Before your clients can get content from the cloud-based distribution point, you need to deploy to them the cloud-based distribution point service certificate. Also remember that you need to enable Allow Access To Cloud Distribution Point under Device/User Settings, as shown in Figure 5.13.

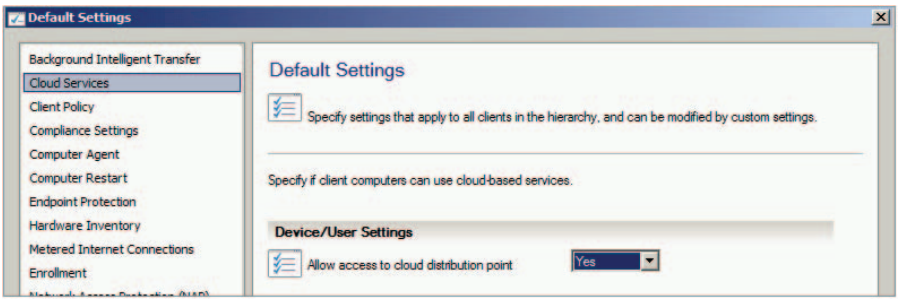


FIGURE 5.13
Client Settings

Configure Name Resolution for Cloud-based Distribution Points

Before your clients can access the cloud-based distribution point, they must be able to resolve the name of the cloud-based distribution point to an IP address that matches the service in Windows Azure. Clients do this is two stages:

1. Clients map the service name that you provided with the Configuration Manager cloud-based distribution point service certificate to your Windows Azure service fully qualified domain name (FQDN). This FQDN contains a GUID and the DNS suffix of cloudapp.net. The GUID is automatically generated after you install the cloud-based distribution point. You can see the full FQDN in the Windows Azure Management Portal, by referencing the SITE URL in the dashboard of the cloud service. An example site URL is `http://f83e1229e5384427b325e44a.cloudapp.net/`.
2. Clients resolve the Windows Azure service FQDN to the IP address that Windows Azure allocates. This IP address can also be identified in the dashboard for the cloud service in the Windows Azure portal and is named PUBLIC VIRTUAL IP (VIP) ADDRESS.

To map the service name that you provided with the Configuration Manager cloud-based distribution point service certificate (for example, CM2012R2CloudDP.cloudapp.net) to your Windows Azure service FQDN (for example, f83e1229e5384427b325e44a.cloudapp.net), DNS servers on the Internet must have a DNS alias (CNAME record). Clients can then resolve the Windows Azure service FQDN to the IP address by using DNS servers on the Internet.

The Bottom Line

Test cloud distribution points before going into production. Before you go into production with cloud-based distribution points, you should test the service to make sure it meets your needs. The tools required for testing and the trial service are free.

> **Master It** Creating a cloud distribution point is easy, but there are prerequisites that need to be met. You will need a Windows Azure account and Visual Studio to create the management certificate.

Control cloud distribution points usage costs. Don't set and forget your cloud-based distribution points. Monitor its usage so you can control your costs. Monitoring usage will also help you determine when it is time to scale up.

> **Master It** Make sure you have control of the charges associated with data transfers from your Windows Azure subscription.

Simplify your hierarchy. Since the early development stages of Configuration Manager 2012, Microsoft has been telling us to flatten or simplify our Configuration Manager hierarchies. Cloud-based distribution points provide you with another opportunity to do so.

> **Master It** Flatten your Configuration Manager hierarchy. There are probably site roles that could be decommissioned by deploying cloud-based distribution points.



Chapter 6

Client Installation

Once you have the Configuration Manager sites and site servers installed and configured, the next logical step is to plan the client deployment. The client deployment success rate very much depends on your knowledge of the internal network infrastructure combined with the ability to understand the components involved in the process. Once you fully understand the process, installing a large number of clients over a short period of time may be no problem. On the other hand, if you do not truly understand the process, installing a single client can be a very time-consuming experience.

No one solution for deploying the Configuration Manager client fits all organizations. Most likely you will find yourself using a mix of the different installation techniques described in this chapter.

This chapter covers the prerequisites for installing clients, a walk-through of the different client installation methods, and information needed for troubleshooting the installation process.

In this chapter, you will learn to

- Configure boundaries and boundary groups
- Select the relevant discovery methods
- Employ the correct client installation methods
- Manage Unix/Linux and Mac devices
- Ensure client health

Creating Client Settings

In order to manage a device with Configuration Manager, you must first have the client software installed. Regardless of the device and operating system on that device, we always use the term *client* when we refer to the software on the managed computer that interacts with the Configuration Manager site servers. A client consists of different agents that you can enable or disable. During the installation, the full Configuration Manager client is installed, and you use the Client Settings section of the Administration workspace to control the agent settings and configuration. In Configuration Manager 2012, client settings are global data and thus are no longer separately controlled by each primary site. Furthermore, you can create multiple custom

client settings and assign them to individual collections. As a best practice, you should typically configure custom client settings only as exceptions to the default client settings. There may be several reasons why you would need to configure multiple client settings, for example:

- You want to control who can initiate a remote session against servers.
- You want to disable the remote tools agent on all computers in the HR department.
- You want different inventory frequencies on servers and desktops.

A set of default client settings is always configured when you install Configuration Manager. In Figure 6.1 you can see an example of where two custom client settings have been created and assigned to two different collections. Notice the number in the Deployments column; it indicates the number of collections that are affected by the custom client settings. Figure 6.2 shows the new client settings interface. You can assign your own custom client settings to any user or device collection. The same settings can be assigned to multiple collections, and one collection can have multiple assignments. In the event of a conflict, the custom setting with the lowest Order number will be assigned.

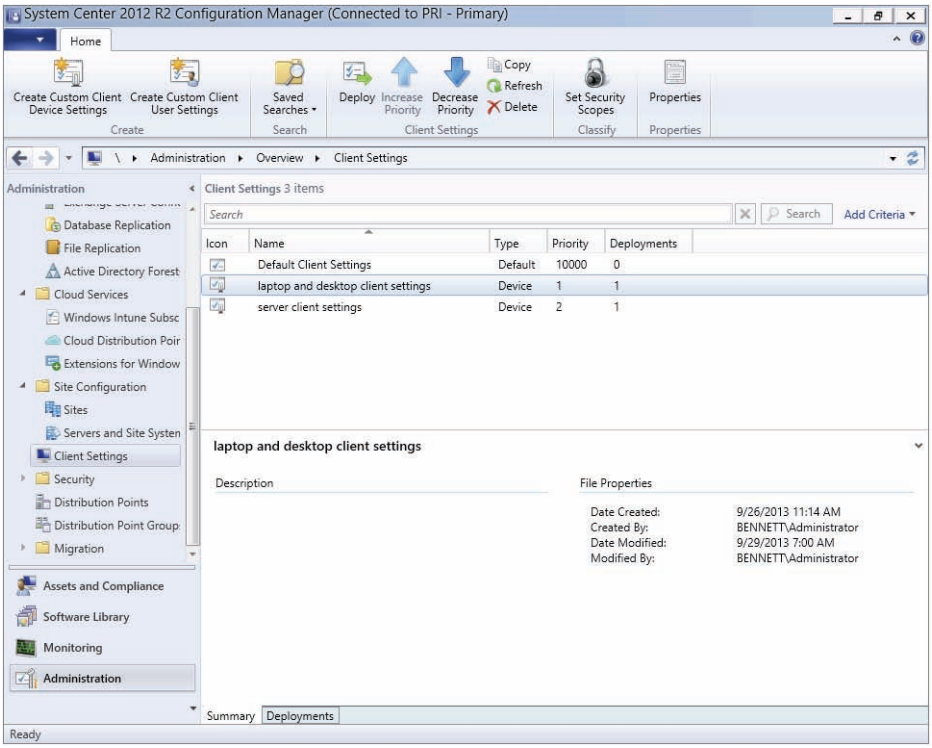


FIGURE 6.1
Client settings

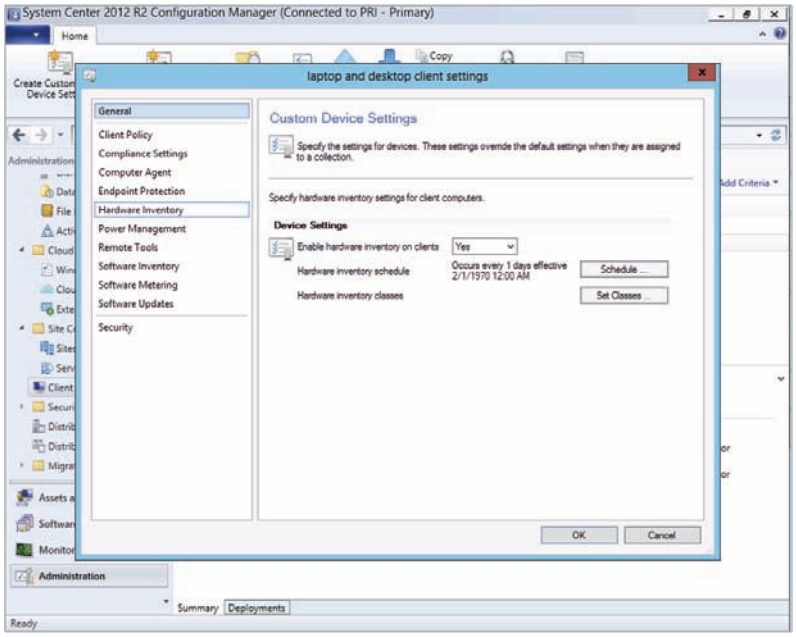


Figure 6.2
Creating custom client settings

Real World Scenario

Configure Different Custom Client Settings for All Servers

As the Configuration Manager administrator, you have been requested to ensure that only members of the global group Server Administrators can use Remote Tools on servers. Follow these steps to do so:

1. Open the Configuration Manager 2012 administrative console.
2. Select the Administration workspace and browse to Client Settings.
3. On the Home tab of the ribbon, click Create Custom Client Device Settings.
4. Type **Remote settings for servers** in the Name column.
5. From the list of custom settings, select Remote Tools.
6. In the left column, select the Remote Tools settings and click Set Viewers.
7. Click the yellow starburst and in the New Permitted Viewer window enter the name of the user or group that should be given access in the User or group name field. This should be in the form of domain\group name (or domain\user name). For example, **Contoso\Server Administrators**.
8. Click OK three times.

   Notice the number shown under Permitted Viewers.
9. Click OK to save the custom client settings.
10. Back in the administrative console, select the newly created custom settings, and click Deploy on the ribbon.
11. Select the All Servers device collection, and click OK.

The individual client agent settings will be discussed in detail in later chapters. Figure 6.2 shows a client settings group that includes several of the available client actions. You can view the list of all possible settings by selecting the Default Client Settings and selecting Properties in the Ribbon. Here is a short description of each of the agent settings:

Background Intelligent Transfer This setting allows you to control the BITS protocol. BITS is the protocol being used by the client when it is downloading and uploading information to the management point and also when it is downloading packages from the distribution points.

Cloud Services This setting determines whether client computers are allowed to access cloud distribution points.

Client Policy The Client Policy settings control how often the client agent will contact the management point for a policy refresh:

- Client Policy Polling Interval (Minutes) defines how often the client will request a new machine policy. It can be any value between 3 minutes and 1440 minutes. Best practice (and the default value) is 60 minutes. Notice that unlike previous versions, Configuration Manager 2012 does not use policies when offering new applications to end users.
- Allow User Policy Request From Internet Clients: Use this setting if you have any Internet-facing site systems and you want to support user-centric scenarios for Internet-based clients.

Compliance Settings This option is used to enable the settings-management feature formerly known as Desired Configuration Management in Configuration Manager 2007.

Computer Agent Here you define most of the basic Configuration Manager client settings:

- Deployment Deadline settings are used to control when users will be reminded about future deployments.
- Default Application Catalog Website Point: Use this setting to define how clients will connect to the Application Catalog. It can either be automatic, a specific server, or a specific website. If you select Automatic, the management point will supply the client with a random catalog, which is not guaranteed to be the one nearest the user.
- Add Application Catalog Website To Internet Explorer Trusted Sites Zone will add the selected website to the trusted site zone.
- Organization Name is the name that will be displayed in the Software Center.
- Install Permissions can be configured to control the permissions required to start any deployment on the client. You can choose from All Users, Administrators, Primary Users, or No Users. This setting is particularly valuable when you are controlling terminal servers.
- Suspend BitLocker PIN Entry Or Restart is used to control whether you want to suspend the PIN requirements after running a deployment that requires a system restart.
- Agent Extensions Manage The Deployment Of Applications And Software Updates: Enable this setting only if required by a vendor or if you use the SDK to manage client agent notifications.

- PowerShell Execution Policy: By default PowerShell scripts will run in the context of a service. If you want to run a PowerShell script within a task sequence, you should select Bypass, which is the same as running the PowerShell script unrestricted.
- Show Notifications For New Deployments controls the default UI experience for the logged-on user when a deployment is received or about to start.

Computer Restart This setting allows you to control when restart notifications are shown.

Endpoint Protection Here you enable or disable the System Center Endpoint Protection agent. The settings are configurable only when you have enabled the Endpoint Protection Site System role:

- Manage Endpoint Protection Client On Client Computers: Configure this setting to True to start managing Endpoint Protection in the hierarchy.
- Install Endpoint Protection Client In Client Computers: When this setting is True, the Endpoint Protection client will automatically be installed. Notice that the client is already deployed during the initial Configuration Manager client installation.
- Automatically Remove Previously Installed Antimalware Software Before Endpoint Protection Client Is Installed: When this is True, an attempt to uninstall some predefined antimalware application will be performed.
- Suppress Any Required Computer Restart After The Endpoint Protection Client Is Installed: If configured to True, no restart will be performed, not even if a previous antimalware application is uninstalled first.
- Allowed Period Of Time Users Can Postpone A Required Restart To Complete The Endpoint Protection Installation (Hours): This option is configurable only if the setting to suppress computer restart is False. The number of hours will be the maximum number of hours a restart can be postponed by the user before a restart of the computer will be forced.
- Disable Alternate Sources (Such As Microsoft Windows Update, Microsoft Windows Server Update Services, Or UNS Share) For The Initial Definition Update On Client Computers: Configure this setting to False if you want to allow multiple update sources to be considered for the first definition update.

Hardware Inventory This option is used to scan for and report hardware installed on the computer. You can specify custom agent settings for different collections but only define hardware to collect in the default client settings. Unlike Configuration Manager 2007, there is no unique `sms_def.mof` file per site; instead you use the Custom Client Settings interface to specify the inventory data classes.

Metered Internet Connections This setting can be used to control costs if client computers are utilizing an Internet service provider that charges based on the amount of data that is used.

Enrollment This setting provides configuration options for enrolling mobile devices and Mac computers. It can be used to define the polling interval for mobile device legacy clients as well as defining whether or not end users are allowed to enroll mobile devices and Mac computers.

Network Access Protection (NAP) Use this option to enable Network Access Protection compliance on systems as well as to schedule when scans will occur. Notice that NAP requires that you have installed and configured Network Policy and Access Services in Windows Server 2008 (or higher).

Power Management This setting enables power management for all clients in the hierarchy and allows you to control whether end users can exclude their own devices from being part of a power management configuration. You configure each of the Power Management settings by collection.

Remote Tools This is used to control the Remote Tools and Remote Assistance settings for Windows XP and later systems.

Software Deployment Use this option to configure whether notifications should be shown when deployments are about to run. Schedule Re-evaluation For Deployments determines how often the Configuration Manager client will trigger the re-evaluation process. The process will automatically install required software that is not already installed and remove software that is supposed to be uninstalled.

Software Inventory This option is used to discover what software is installed on the computer. You can control which file types the agent will scan for and where. Furthermore, you can use the settings to collect software files. Collected files are not stored in the database but will be stored on the site server. Even though it might be tempting to collect files, you should think twice before enabling this feature because it can easily lead to network congestion.

Software Metering This option enables software metering and controls how often clients will upload the software-metering data from WMI to the management point.

Software Updates This setting enables software updates, controls how often clients will perform a scan for software updates, and determines whether or not all required updates should be installed upon the deployment deadline.

State Messaging This setting controls how often state messages are forwarded from the client to the management point.

User And Device Affinity This setting controls the calculations that are being used to determine when a user(s) is being considered a primary user(s) for a device.

Supported Operating Systems

The following are the more common operating systems that are supported for the Configuration Manager client. The complete list of supported operating systems is available at `http://technet.microsoft.com/en-us/library/gg682077.aspx`. (Mobile devices will be discussed in detail in Chapter 16, "Mobile Device Management.")

Windows:

- Windows XP Professional Service Pack 3 for X86 (SP2 for x64)
- Windows Vista Business/Enterprise/Ultimate Edition SP2
- Windows 7 Professional/Enterprise/Ultimate
- Windows 8 Professional/Enterprise

- Windows 8.1 Professional/Enterprise
- Windows Embedded Standard 2009 X86
- Windows Embedded POS Ready 2009 X86
- WEPOS 1.1 SP3 X86
- Windows XP Embedded SP3 X86
- Windows Embedded Standard 7 X86 and X64
- Windows Server 2003 Web Edition SP2, X86
- Windows Server 2003 Standard/Enterprise/Datacenter Edition SP2
- Windows Server 2003 R2 SP2
- Windows Storage Server 2003 R2 SP2
- Windows Server 2008 Standard/Enterprise/Datacenter SP2 and Server Core
- Windows Server 2008 R2 Standard/Enterprise/Datacenter and Server Core
- Windows Server 2012 Standard/Datacenter and Server Core
- Windows Server 2012 R2 Standard/Datacenter and Server Core

The following are the prerequisites for Windows-based clients:

- Users who use the Application Catalog must configure Internet Explorer to exclude the ActiveX control `Microsoft.ConfigurationManager.SoftwareCatalog.Website.ClientBridgeControl.dll` from ActiveX filtering and allow it to run in the browser.
- Microsoft Windows Installer version 3.1.4000.2435 or later
- Microsoft Background Intelligent Transfer Service (BITS) version 2.5

The following are the prerequisites for Windows-based clients downloaded during the client installation:

- Microsoft Windows Update Agent version 7.0.6000.363 or later
- Microsoft Core XML Services (MSXML) version 6.20.5002 or later
- Microsoft Remote Differential Compression (RDC)
- Microsoft .NET Framework 4.0 Client Profile
- Microsoft Silverlight 4.0.50524.0
- Microsoft Visual C++ 2005 Redistributable version 8.0.50727.42
- Microsoft Visual C++ 2008 Redistributable version 9.0.30729.4148
- Windows Imaging APIs 6.0.6001.18000
- Microsoft Policy Platform 1.2.3514.0
- Microsoft SQL Server Compact 3.5 SP2 components

Configuration Manager 2012 SP1 and R2 also provide client support for Linux/Unix computers as well as Macintosh computers. The following are the supported operating system versions for these platforms:

Linux/Unix:

- Red Hat Enterprise Linux (RHEL) Version 4 (x86 & x64), Version 5 (x86 & x64), Version 6 (x86 & x64)
- Solaris Version 9 (SPARC), Version 10 (SPARC & x86), Version 11 SP1 (x86 & x64)
- SUSE Linux Enterprise Server Version 9 x86, Version 10 SP1 (x86 & x64), Version 11 SP1 (x86 & x64)
- CentOS Version 5 (x86 & x64), Version 6 (x86 & x64)
- Debian Version 5 (x86 & x64), Version 6 (x86 & x64), Version 7 (x86 & x64)
- Ubuntu Version 10.4 LTS (x86 & x64), Version 12.4 LTS (x86 & x64)
- Oracle Linux Version 5 (x86 & x64), Version 6 (x86 & x64)
- HP-UX, Version 11iv2 (IA64 & PA-RISC), Version 11iv3 (IA64 & PA-RISC)
- AIX Version 5.3 (Power), Version 6.1 (Power), Version 7.1 (Power)

Macintosh:

- Mac OS X 10.6 (Snow Leopard)
- Mac OS X 10.7 (Lion)
- Mac OS X 10.8 (Mountain Lion)

Discovering Network Objects

Discovery is the process by which Configuration Manager finds objects in the computer infrastructure and keeps them up to date in the Configuration Manager database. Objects can be users, groups, and computers. All discovery processes will generate one data discovery record (DDR) for each discovered object. For an administrator it is nice to know how many computers you have (and where they are) before you start deploying clients. To find out, you must understand the different discovery methods and when they should be used. Discovery also plays an important part in creating the collections that will support features like application deployment, updates deployment, and operating system deployment.

The only discovery method enabled by default is Heartbeat Discovery, described in a later section. Before configuring any other discovery method, you must ask yourself a few basic questions:

- What is being discovered by the method?

  This is essential knowledge before configuring any of the methods. If you do not understand what's being discovered, chances are that you will discover the wrong information.

- Why do you need the data?

  If you can't answer this question, most likely you do not need to configure the discovery method.

- How often do you need to refresh the discovery data?

  Configuration Manager 2012 natively supports delta discovery, which eliminates the reason for running frequent full discovery processes.

- What is the duration of the discovery process?

  Not knowing the duration of each discovery method has often resulted in backlogs and incorrect discovery schedules. Having knowledge about the log files generated by each discovery process can give you precise data and help you configure the correct schedules.

- What is the impact of configuring the method?

  The discovery methods use different techniques to gather a data discovery record (DDR). Active Directory methods will query the nearest domain controller, whereas Network Discovery uses protocols like RIP and OSPF to get the information.

  To configure discovery methods, perform the following steps:

1. Open the Configuration Manager administrative console.
2. Select the Administration workspace, navigate to Hierarchy Configuration, and choose Discovery Methods.
3. You can modify each of the discovery methods by selecting the discovery method and choosing Properties from the ribbon.

Active Directory Discovery Methods

Each of the Active Directory discovery methods requires a target and a schedule. The target can be a single object, an organizational unit (OU), a security/distribution group, or an entire domain. While it might not make much sense to search for a single object, specifying individual OUs or groups versus the entire domain is often considered a best practice. Especially in the pilot phase, it is an easy way to limit the number of objects you are working with. A new feature in Configuration Manager 2012 allows you to specify the account being used to run the discovery process. If none is specified, the process will run under the security context of the site server. In order to run a successful discovery, the account you specify must have Read permission on the object.

Figure 6.3 shows the Active Directory Container field that you use to define the locations where you want to search. When you click Browse, you will see the dialog shown in Figure 6.4. This dialog allows you to select the criteria for the LDAP query. You can select any container or OU within the tree view. Unlike with previous versions of Configuration Manager, you can now browse to other domains and forests.

Figure 6.3
New Active Directory Container search criteria

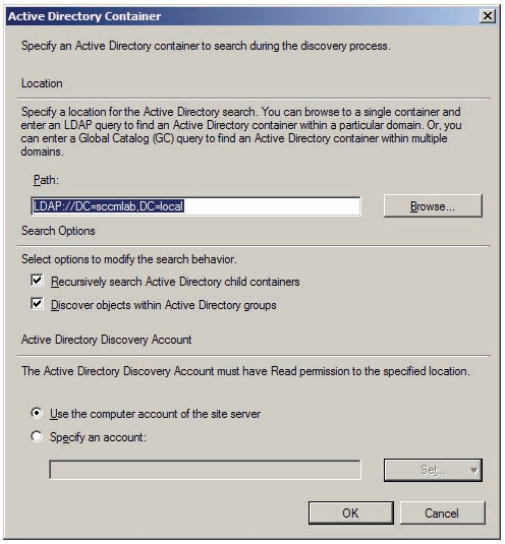
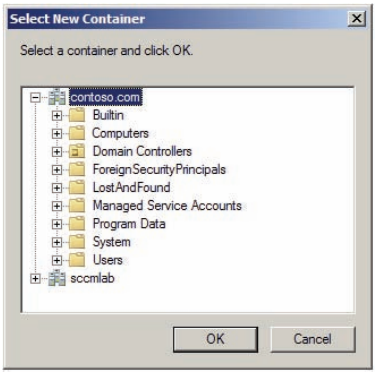


Figure 6.4
The Select New Container dialog box





Real World Scenario

Discovery Paths and Active Directory Organizational Units

It is important to know that Configuration Manager will query all objects in the specified paths every time. If you delete an old computer object from the Configuration Manager database but not from Active Directory, the same computer object will be added to the Configuration Manager database after the next discovery process unless you have configured the option to exclude computer objects that have not recently logged on or changed their password. Failure to exclude computers can have an effect on the automatic client push installation attempts because Configuration Manager will initiate a client push attempt on computers that do not have the client installed. These might be the most important reasons why you should plan the discovery processes carefully; make sure that you have an OU structure in Active Directory where you can store objects that are no longer active and exclude those OUs from the specified LDAP path. Failure to do so might lead to errors related to failed client push installation attempts and discovery of unwanted objects.

Once you choose the start location for the query, the default behavior of the query is to search all of the child objects beneath the starting point. If you do not want to search through the child OUs, you can clear the check box labeled Recursively Search Active Directory Child Containers. This is a good way to limit the data returned from the query.

The option Discover Objects Within Active Directory Groups is especially useful in scenarios where you want the Active Directory System Group Discovery method to find computer objects within Active Directory groups. Many organizations have a unique OU where they store computer groups.

Figure 6.5 shows all discovery methods available in a primary site. Let's look at each of these methods in detail.

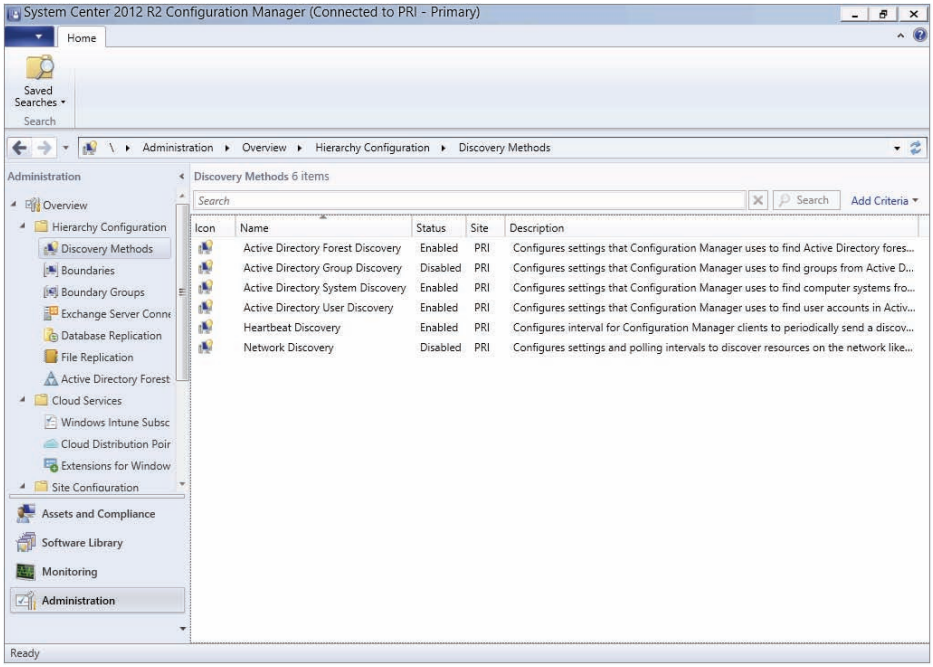


Figure 6.5 Discovery methods

Active Directory Forest Discovery

This discovery method is new to Configuration Manager 2012 and can be very helpful in environments where the Configuration Manager administrator is not always informed about IP infrastructure changes. The method returns information about domains, IP ranges, and Active Directory sites. Furthermore, as shown in Figure 6.6, you can configure the method to automatically create boundaries for the objects being discovered (IP ranges or Active Directory sites only), thus saving yourself hours of work.

By default the discovery process runs once a week and will only discover those forests that are created as Active Directory Forest objects in the Administration workspace. The local forest is automatically created as part of the site installation process. Figure 6.7 shows how you can specify a new forest using an account from the target forest.

You can monitor this discovery process by reading the `ADForestDisc.log` on the site server.

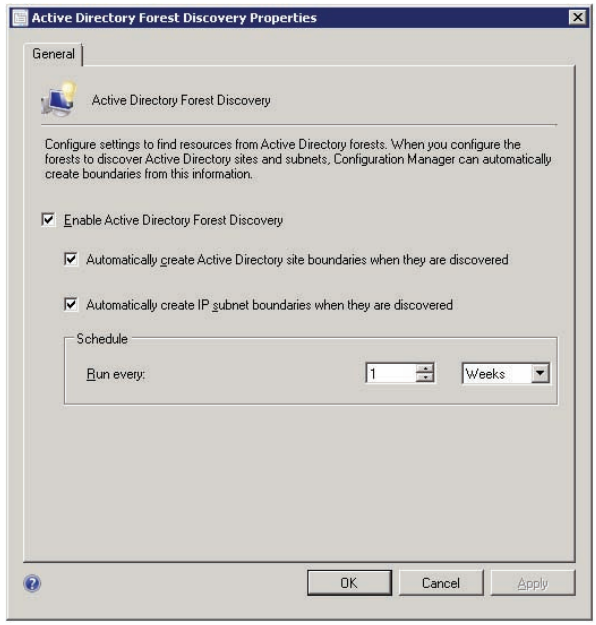


FIGURE 6.6
Configuring Active Directory Forest Discovery

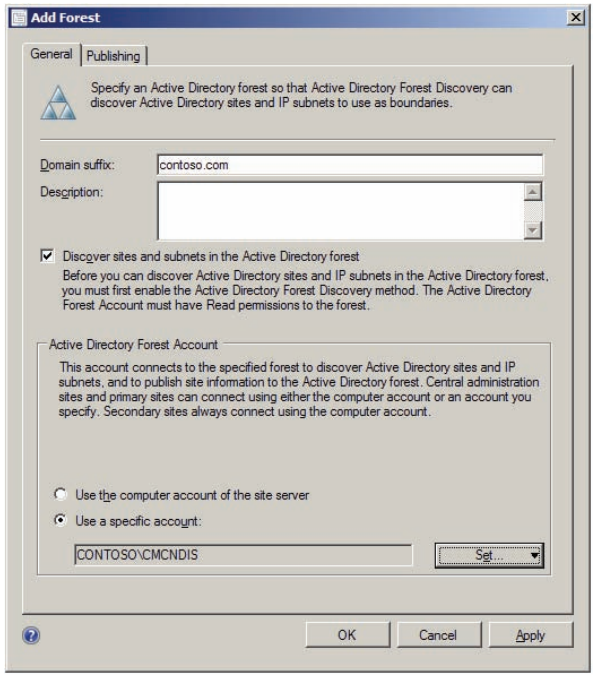


FIGURE 6.7
Defining a new Active Directory forest

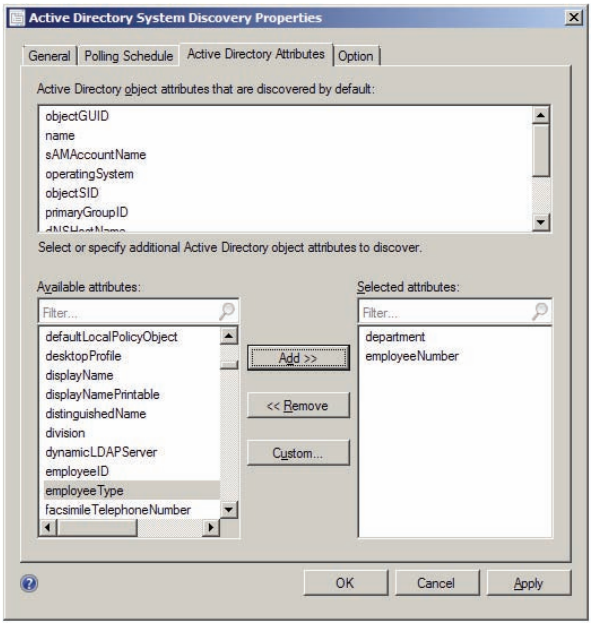
Active Directory System Discovery

This is the key discovery method for finding devices. In essence you configure one or more LDAP paths to Active Directory and query a domain controller for all objects in those paths. The device attributes returned by the domain controller depend on what you have configured. By default these attributes will be returned:

- ObjectGUID
- Name
- SAMAccountName
- ObjectSID
- PrimaryGroupID
- DNSHostName
- UserAccountControl
- LastLogonTimestamp
- DistinguishedName

In Figure 6.8 you see an example where custom attributes have been specified. Attributes can be specified for AD System Discovery and AD User Discovery. The information you specify will be added to the discovery data and used in queries and reports like any other discovery information. You can monitor this discovery process by reading the `ADSysDis.log` on the site server.

Figure 6.8
Custom Active Directory system attributes



Active Directory User Discovery

This discovery method is not used at all in the client deployment process but plays an important part of the user-centric application model. With the method enabled you will get a list of users to whom you can target different deployments such as applications. By default these attributes will be returned:

- ObjectGUID
- Name
- UserAccountControl
- SAMAccountName
- ObjectSID
- PrimaryGroupID
- DNSHostName
- Mail
- DistinguishedName
- UserPrincipalName

You can monitor this discovery process by reading the `ADusrdis.log` on the site server.

Active Directory Group Discovery

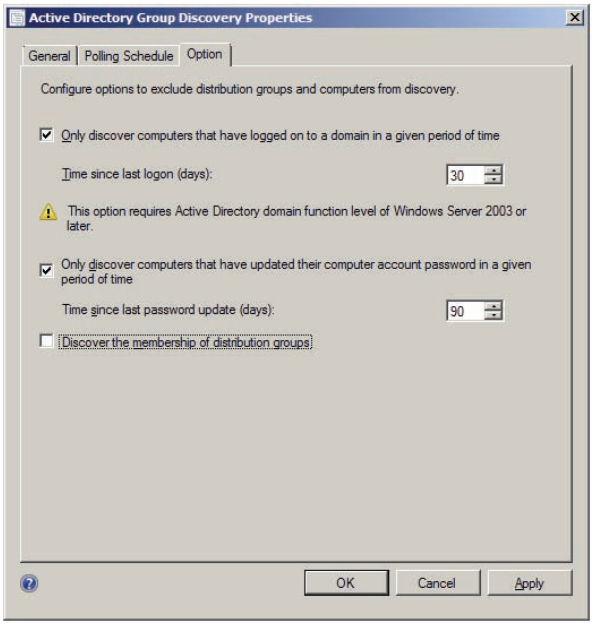
This discovery method will discover any local groups, global groups, and universal security groups. You can search for objects within a specific group or perform the search for all groups in a specific location. The information is not really used in a client installation scenario. But once you have the client deployed, you will find the Active Directory security group very useful, especially in user target deployments. You can limit the number of objects returned in the discovery process by configuring the values on the Option tab, as shown in Figure 6.9. Notice that discovering only computers that have logged on to a domain within a specified number of days requires that the domain function level be at least Windows 2003.

You can monitor this discovery process by reading the `ADsgdis.log` on the site server.

Heartbeat Discovery

This discovery method is enabled by default and differs from the other methods. It is the responsibility of the client to initiate the discovery process. Failure to do so can result in unwanted client installation attempts and cause the client to be marked as inactive in the Configuration Manager console. The discovery process will not discover any new objects; instead it rediscovers existing objects. You can look at this method as a way to send a keep-alive package from the client to the management point. The heartbeat record is used for the following purposes:

FIGURE 6.9
Option tab for group discovery



- Determine whether a client is marked active or inactive.
- Update the Client column from No to Yes in the console when the client is installed.
- Re-create the client in a database if you accidently deleted the object.
- Have an impact when the Clear Install Flag site maintenance task will delete the client install flag in the database. If the install flag is removed and automatic client push is enabled, a new client installation attempt will begin.

How often should you run the discovery method? By default clients will send an updated DDR to the management point every seven days, and you can change this to occur more frequently, perhaps daily, if needed to meet your requirements. As with any Configuration Manager changes, monitor the environment for any performance or file backlog issues if you make changes to the default settings. These are some of the attributes that will be returned:

- ClientInstalled
- ClientType
- ClientID
- ClientVersion
- NetBIOSName

- IPSubnet
- Domain
- ADSiteName
- IPAddress
- MACAddress

You can monitor this discovery process by reading the `InventoryAgent.log` on the client.

> **Heartbeat Discovery and Modifying Computer Names**
>
> The Heartbeat Discovery process is responsible for updating changes in the computer name to the database. If you are starting a process where you need to rename a large number of computers, consider modifying the default schedule from seven days to a more frequent interval.

Network Discovery

Let me start by saying this: Run the Network Discovery method only when no other discovery method can find the needed resources. It is considered to be the "noisiest" method and will use protocols like RIP or OSPF to discover objects. Most often you'll need to use this method only if you have a number of workgroup clients in your environment. Network Discovery is used to discover many different types of objects. Not only can you find computers that are on the network, but you can discover any device that has an IP address as well.

You can monitor the Network Discovery process by reading the `Netdisc.log` on the server.

Discovery Scheduling Options

Each method also has a way of scheduling when the discovery will run. For the Active Directory discovery methods, the Polling Schedule tab resembles Figure 6.10 (in this case Active Directory System Group Discovery). The schedule determines when the site server will initiate a full discovery. You can also configure delta discovery. Delta discovery runs by default every 5 minutes and will only discover any changes made to the objects. Unlike in Configuration Manager 2007 R3, the process will discover when you modify existing objects, such as adding an existing computer account to an existing group. Using delta discovery along with the collection property Use Incremental Updates For This Collection, all changes will be reflected in the collection within 10 minutes: 5 minutes for the delta discovery and 5 more minutes for the incremental collection update.

If you need to modify the schedule, click the Schedule button to display the Custom Schedule window.

The Heartbeat Discovery method schedule is found on the General tab, as shown in Figure 6.11. Notice that you can set only a simple schedule for the Heartbeat; your options are much more limited than with the Active Directory methods.

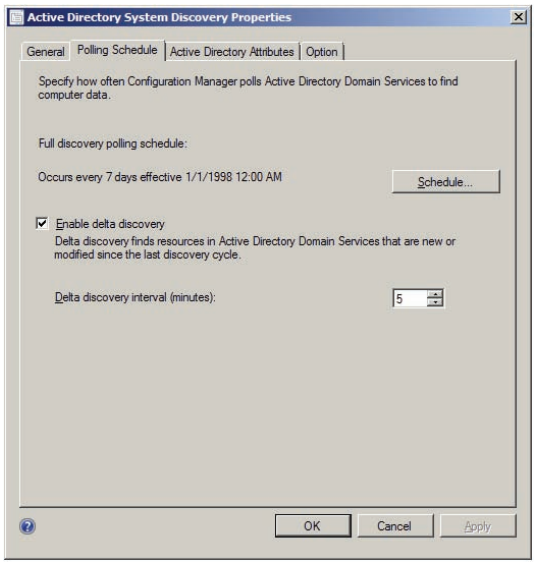


Figure 6.10
Polling Schedule tab for a discovery method

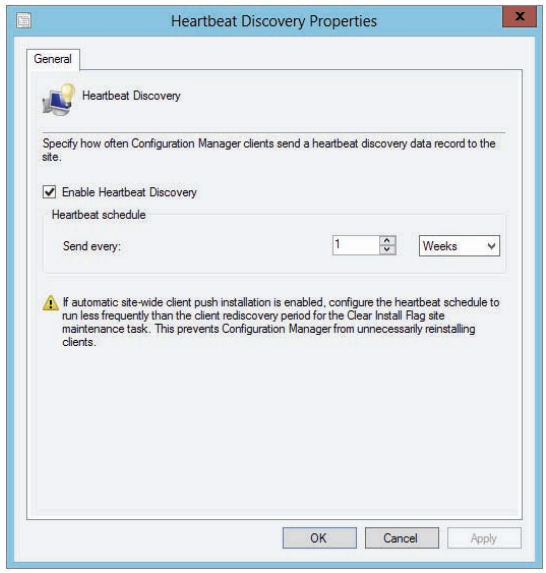


Figure 6.11
The Heartbeat Discovery General tab

You can create multiple schedules for the Network Discovery method, as shown in Figure 6.12. Configuring the options in the Custom Schedule dialog shown in Figure 6.13 gives you a lot of control over scheduling the Network Discovery agent. Because of the time required for the network searches, you may want to configure a maximum runtime.

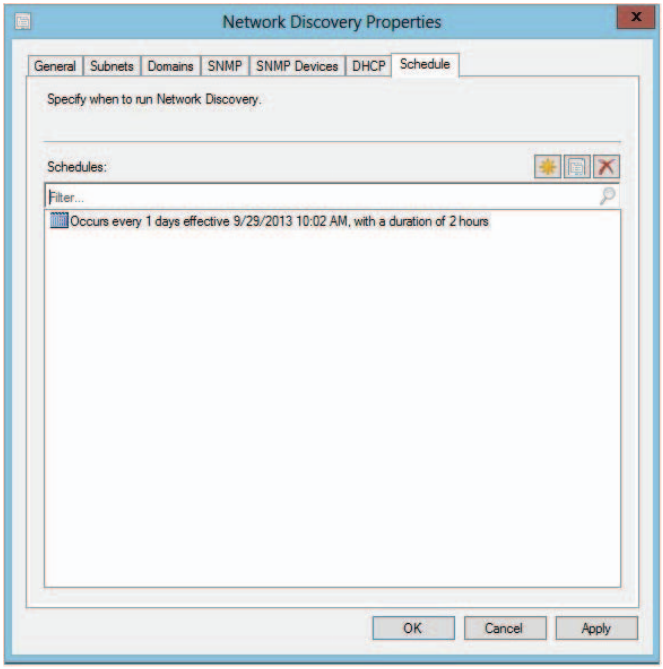


Figure 6.12
The Network Discovery Schedule tab

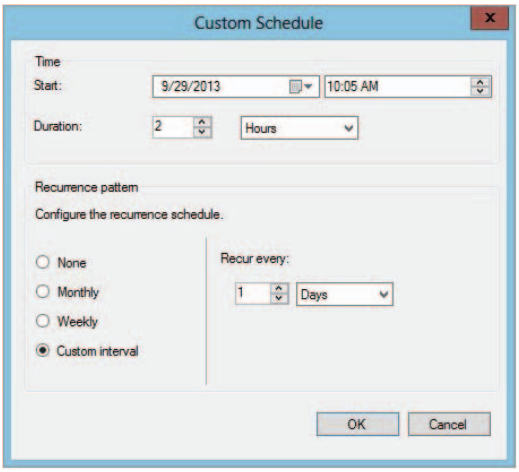


Figure 6.13
The Custom Schedule dialog for Network Discovery

Configuring Boundaries and Boundary Groups

After a client has been installed, it must be assigned to a Configuration Manager 2012 R2 site before it can be managed. Once assigned, the client will start receiving the default client policies, using the local resources of the site such as management points, distribution points, and software update points. During the installation, you can configure command-line

properties to automatically assign the client a fixed site code or let an auto-assignment process begin. Note that clients will never be assigned to secondary sites, only primary sites.

Configuring boundaries has long been the way you assigned a client to a Configuration Manager/SMS client site. This has changed in Configuration Manager 2012, where a new feature has been introduced to control the assignments: boundary groups. In essence you still use boundaries, but they have no real value until they have been added to a boundary group. A boundary group is basically a collection of individual boundaries grouped together for one or two purposes:

Site Assignment Used to control which sites clients are assigned to

Content Lookup Used to control which distribution points will be used by the client

Figure 6.14 and Figure 6.15 show a site boundary added to a boundary group that is configured for site assignment.

Boundaries are basically address ranges; the following range types are supported:

- IP subnet
- Active Directory site
- IPv6 prefix
- IP address range

Even though all four boundary types are supported, there will be scenarios where one or more of the types will not work correctly. There are known issues with IP subnets and network IDs that might cause clients not to be assigned even if they fall within the boundary defined. Furthermore, AD site boundaries are not supported in IP supernetting environments. If you experience problems, you can always configure IP ranges.

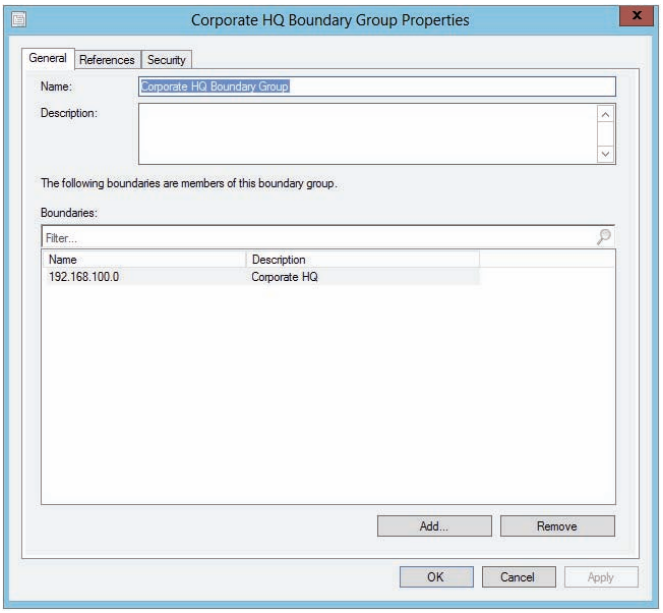


Figure 6.14 Boundary group with a list of boundaries

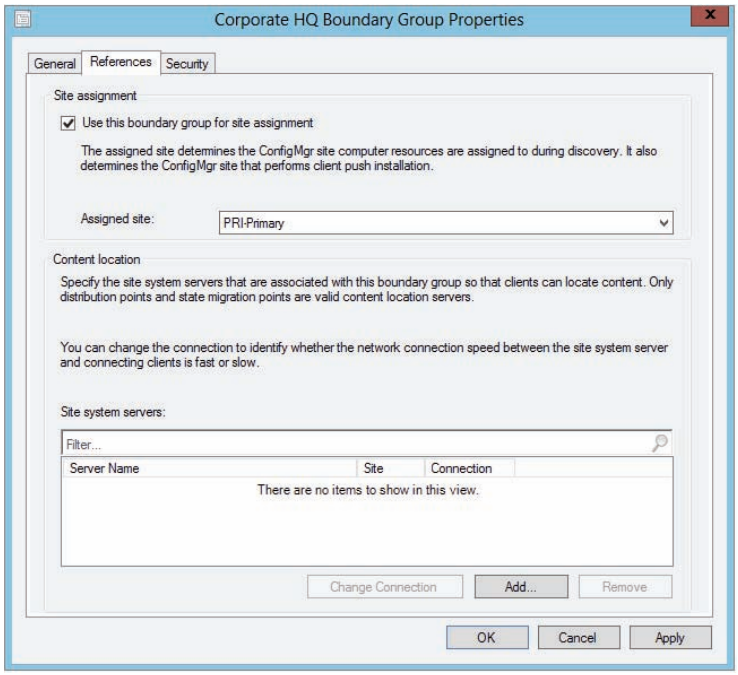


FIGURE 6.15
Boundary group configured for site assignment



Real World Scenario

CONFIGURING A BOUNDARY AND A BOUNDARY GROUP

As the Configuration Manager administrator, you have been requested to create an AD boundary and ensure it is used to assign clients to the primary site. Follow these steps:

1. Open the Configuration Manager 2012 administrative console.
2. Select the Administration workspace and browse to Overview ➢ Hierarchy Configuration ➢ Boundaries.
3. On the ribbon click Create Boundary.
4. Type **HQ** in the Description field, and under Type select Active Directory Site.
5. Click Browse, select the Active Directory site, and click OK.
6. Click OK to create the boundary.
7. Navigate to Boundary Groups, and on the ribbon click Create Boundary Group.
8. In the Name field type **HQ**, click Add, select the newly created boundary, and click OK.
9. Select the References tab.
10. Check the box Use This Boundary Group For Site Assignment. Select a primary site and click OK.

Client Installation Methods

As an important part of your client deployment planning, you need to ask yourself a few questions:

- How are you going to deploy the client?

  Basically you can choose between a manual installation and an automatic installation. The automatic installation method comes in different flavors.

- Where are you deploying the client?

  You need to know which environments need a client. Many organizations plan only for client support in the local domain just to realize later in the process that they also need to support workgroup clients, clients in DMZ, and clients in other forests.

- When do you want to deploy the client?

  You need to decide whether you want to deploy all clients at once or in a controlled manner.

You have several different deployment methods to choose from; most organizations find themselves using a mix of different methods. It is important to know that there is no right or wrong method, but methods used in different scenarios have different requirements. Regardless of the installation method, you need to know the different command-line properties and when to use them. Gaining knowledge about the command-line properties will ensure that you can install clients in different environments such as workgroups, other forests, and DMZs.

Command-Line Properties

Several command-line properties are used to control the installation. Before you start the deployment, you will need to know two things:

- What command-line properties are you going to use?
- How are you going to provision the command-line properties?

The installation process will always run `ccmsetup.exe` and `client.msi`; both of these processes can be controlled using command lines. Any needed prerequisites will be installed and controlled by `ccmsetup.exe`. When you specify command-line properties, you should do so like this:

```
CCMSetup.exe [CCMsetup properties] [client.msi setup properties]
```

For an updated list of command-line properties, you should look at the TechNet article at this URL:

`http://technet.microsoft.com/en-us/library/gg699356.aspx`

The following are `ccmsetup.exe` command-line properties:

`/source` The `/source` switch is used to identify the location of the `client.msi` installer file. You can specify the switch multiple times to provide additional source file locations to provide for redundancy. Usage: `ccmsetup.exe /source:folderpath`.

/MP The /MP switch is used to specify the management point that will be used as a source location. As with the /source switch, you can specify multiple management points by including the switch multiple times. The setting is not used to control the management point that will be used during the site assignment process. Usage: ccmsetup.exe /MP:*Server*.

/retry:<minutes> The /retry switch is used to retry values used to determine how often a client will try to download the installation files. The client will attempt to download the files until it reaches the values specified in downloadtimeout. Usage: ccmsetup.exe /retry:30.

/downloadtimeout:<minutes> The /downloadtimeout switch controls the number of minutes the ccmsetup process attempts to download the needed client installation files. By default the ccmsetup process will try downloading files for one day. Usage: ccmsetup / download timeout:120.

/noservice The /noservice switch is used to specify that the logged-in user's account is the service account for the installation of the client. For this switch to work, the user account will need to have rights to install software; otherwise the installation will fail. Usage: ccmsetup / noservice.

/Service The /Service switch is used to install the client software using the security context of the local system account. For this to work, Active Directory has to be in use within your network, and the computer's Active Directory account must have access to the installation directory where the client installation files are stored. Usage: ccmsetup /Service.

/Logon The /Logon switch is used to determine if a Configuration Manager client exists on the system. If a Configuration Manager 2012 client is already installed, the installation process will stop. Usage: ccmsetup.exe /Logon.

/forcereboot The /forcereboot switch is used to determine if the ccmsetup process needs to perform a restart of the computer in order to finish the installation. Usage: ccmsetup.exe /forcereboot.

/BITSPriority:<Priority> The /BITSPriority switch controls the bits download priority when downloading the client installation files. You can specify these values:

- Foreground
- High
- Normal
- Low

Usage: ccmsetup.exe /BITSPriority:Foreground.

/Uninstall The /Uninstall switch is used to silently uninstall the Configuration Manager client. Usage: ccmsetup.exe /Uninstall.

/UsePKICert The /UsePKICert switch is used to specify that the client will use a PKI certificate that uses client authentication for communication. If no certificate can be found, the client will use a self-signed certificate and communicate using HTTP. Usage: ccmsetup.exe /UsePKICert.

/NoCRLCheck The /NoCRLCheck switch is used to specify that the client will not check the certificate revocation list before establishing HTTPS communication. This example will enable

HTTPS communication and not check for any revocation lists. Usage: `ccmsetup.exe /UsePKICert /NoCRLcheck`.

`/config:<configuration file>` The `/config` switch is used to specify the name of a user-defined configuration file. The configuration file replaces the default `mobileclient.tcf` file. It is a very good idea to modify an existing `mobileclient.tcf` file whenever you want to create a custom configuration file. That way you ensure that the syntax used in the file is correct. Usage: `ccmsetup.exe /config:C:\Windows\ccmsetup\mysettings.txt`.

The following are `Client.msi` command-line properties:

`Patch` This property allows you to apply client patches during the installation. At the time of writing, there are no Configuration Manager 2012 client patches. Usage: `patch=\\Server\Share\clientpatch.msp`.

`CCMALWAYSINF` This property with a value of 1 allows you to determine that the client will always be Internet-based, thus never connecting to the intranet. Usage: `CCMALWAYSINF=1`.

`CCMCERTISSUERS` This property specifies the list of certificate issuers trusted by the Configuration Manager site. Notice that the list is case-sensitive. Usage: `CCMCERTISSUERS= ="CN=CM Root CA; OU=SRV; O=CM, Inc; C=US"`.

`CCMCERTSEL` This property allows you to control the certificate selection criteria used when the client has more than one certificate to choose from. When specifying the criteria you can search for the exact subject name (type **`subject:`** prior to the SN) or a partial match in the subject name (type **`subjectstr:`** prior to part of the subject name, object identifier, or distinguished name). Usage: `CCMCERTSEL="subject:Server1.CM2012.COM"`.

`CCMCERTSTORE` This property allows you to specify an alternative certificate store. You should use the command line only if the certificate is not found in the default store. Usage: `CCMCERTSTORE="CM2012CERT"`.

`CCMFIRSTCERT` With this property configured to 1 the client will automatically select the certificate with longest validity period. Usage: `CCMFIRSTCERT=1`.

`CCMHOSTNAME` This property is used to specify the management point for Internet-based managed clients. Usage: `CCMHOSTNAME="MPServer.CM2012.COM"`.

`SMSPUBLICROOTKEY` This property allows you to specify the trusted root key if, for some reason, it cannot be retrieved from Active Directory. You can open the `mobileclient.tcf` file and copy the trusted root key. Usage: `SMSPUBLICROOTKEY= 02000000A40000525341310 00800000100010081863 32BF592B793C8B7F7C01FB32CB811465DEB71095C4442DE45661CE-25031FE2B6F8D9C1C71C6C0BB335C3B5747035E028C43C35E4F8DF1E0CB8B42289A8B-9F9A3143964817DCC50F0D5DB9A879705AD0F4063F4F30242472A933FE8B452BEE608147D9E-CED79CA9422D5441894D152C54B0ABB920741BA0B5582482EA1231FAB0BD67AAAB-82DEC50BDCE7D91FCCFB2C3F6C03C8C67C31B5F083A98860389E8D2FD93C4C5BAE-6124A4977EA76B5A89AE2917687782783E003C5F215C767782C0F79A1C1E1F4D14E8B693-25C8CC33C574BE774CEA9579AD765A864DB0FBBBBB854D4390473E72014111EFD-FC11DDDF46EF7B1F03EF1D60A3ABDAA52E8868A0`.

`SMSROOTKEYPATH` This property allows you to reinstall the trusted root key from a file. Usage: `SMSROOTKEYPATH="D:\NewRootKey\Rootkey.txt"`.

RESETKEYINFORMATION This property allows you to remove the old trusted root key. This is often used when you move clients from one Configuration Manager site hierarchy to another. Usage: `RESETKEYINFORMATION=TRUE`.

CCMAdmins This property allows you to configure which admin accounts are for the client. If there is more than one account, separate the accounts with a semicolon. Usage: `CCMAdmins=account1;account2;...`.

CCMAllowSilentReboot After the installation is complete, if a reboot is required, this property will cause the machine to reboot without saving any user changes. It needs to be specified only if the silent reboot is to be used. A value of 1 forces the reboot if required. Usage: `CCMAllowSilentReboot`.

CCMDebugLogging This property enables or disables debug logging. A value of 1 enables logging; a value of 0 disables logging. Usage: `CCMDebugLogging=0 | 1`.

CCMEnableLogging This property turns logging on or off. If this property is not included, then logging is disabled. Usage: `CCMEnableLogging=True`.

CCMInstallDir This is the directory where the client software will be installed. Usage: `CCMInstallDir=C:\ConfigMgr`.

CCMLogLevel This property is used to control the amount of logging activity. A value of 0 is verbose logging. A level of 1 logs all information, warning, and error conditions. A level of 2 logs warning and error conditions. A value of 3 logs error conditions only. When included, you must also use `CCMEnableLogging`. Usage: `CCMLogLevel=0 | 1 | 2 | 3`.

CCMLogMaxHistory This property controls the total number of previous log files within the `Logs` directory. When included, you must also use `CCMEnableLogging`. Usage: `CCMLogMaxHistory=NumberOfLogFilesToKeep`.

CCMLogMaxSize This property controls the maximum log file size. When included, you must also use `CCMEnableLogging`. Usage: `CCMLogMaxSize=LogSizeBytes`.

DisableCacheOpt When this property is included in the text box, it disables the Cache configuration setting within the Systems Management properties in Control Panel. Users will not be able to manipulate the settings—only administrators will be allowed to. Usage: `DisableCacheOpt=True`.

DisableSiteOpt When this property is included in the text box, it disables the Site Code configuration setting within the Systems Management properties in Control Panel. Users will not be able to manipulate the settings—only administrators will be allowed to. Usage: `DisableSiteOpt=True`.

SMSCacheDir This property controls the directory where the cache is created. Usage: `SMSCacheDir=directorypath`.

SMSCacheFlags This property can be used to control how much space the cache can occupy and the location where the cache will be stored. When used in conjunction with the `SMSCacheDir` property, you have control over where the cache is stored. The flags are as follows:

SMSCacheFlags=PercentDiskSpace Used to control the size of the cache by allocating the total cache size as a percentage of the disk size. Cannot be used with `PercentFreeDiskSpace`.

SMSCacheFlags=PercentFreeDiskSpace Used to control the size of the cache file by allocating the total cache size as a percentage of the free space on the disk. Cannot be used with `PercentDiskSpace`.

SMSCacheFlags=MaxDrive Used to place the cache on the largest drive in the system. Cannot be used with `MaxDriveSpace`.

SMSCacheFlags=MaxDriveSpace Used to place the cache on the drive with the most free space. Cannot be used with `MaxDrive`.

SMSCacheFlags=NTFSOnly Used to control the placement of the cache drive on volumes formatted with NTFS.

SMSCacheFlags=Compress Used to compress the files within the cache.

SMSCacheFlags=FailIfNoSpace Used to stop installation of the client if there is not enough space on the drive for the cache.

SMSCacheSize This property controls the amount of space in megabytes that the cache will consume or in percentage if used in combination with `PERCENTDISKPACE` or `PERCENTFREE DISKSPACE`. Usage: `SMSCacheSize=`*`CacheSizeInMB`*.

SMSConfigSource This property controls where the configuration source files are stored. Usage: `SMSConfigSource=R | P | M | U`.

SMSDIRECTORYLOOKUP This property controls whether WINS lookup is allowed when the client is trying to locate the management point and the site code. Usage: `SMSDIRECTORYLOOKUP=NOWINS`.

CCMHTTPPort This is the HTTP port used by the client to communicate with the site systems. Usage: `CCMHTTPPort=80`.

CCMHTTPSPort This is the HTTPS port used by the client to communicate with the site systems. Usage: `CCMHTTPSPort=443`.

SMSMP This property is used to configure the initial management point that the client communicates with. Usage: `SMSMP=Server1.CM2012.COM`.

FSP This property specifies that a fallback status point is used. Usage: `FSP=Server1 .CM2012.COM`.

DNSSUFIX This property specifies the DNS domain of the management point. With this option clients will search DNS for the `.srv` record that includes the DNS suffix of the management point. Usage: `DNSSUFFIX=CM2012.COM`.

SMSSiteCode This property controls the site code that is assigned to the client. Usage: `SMSSiteCode=Auto |` *`SiteCode`*.

CCMEVALINTERVAL This property controls how often in minutes the client evaluation process runs. By default the process is configured to run once a day. Usage: `CCMEVALINTERVAL=1440`.

CCMEVALHOUR This property controls when the client evaluation process runs (by the hour). By default the process is configured to run at midnight. Usage: `CCMEVALHOUR=14`.

For example, suppose you wanted to push the client to systems, using the following options:

- Install the cache in the `\Cache` directory on the largest drive.
- Enable verbose logging.
- Keep five log files.
- Automatically discover the site code.

Your entry within the Property text box would look like this:

```
SMSSITECODE=AUTO SMSCACHEDIR=CACHE SMSCACHEFLAGS=MAXDRIVE
SMSENABLELOGGING=TRUE
CCMLOGLEVEL=0 CCMLOGMAXHISTORY =5
```

Provisioning Command Lines

You can provision command lines in three different ways:

- Manually type the command lines during the installation.
- Publish them to Active Directory.
- Configure a Group Policy with the `ConfigMgrInstallation.adm` template.

If the AD schema is extended, you can type the command lines in the Installation Properties for the client push installation method. All properties you enter here will be published to Active Directory and used by any client that can access Active Directory during the installation. Notice that this applies only if you start the installation using `ccmsetup.exe` with no other command lines.

For those scenarios where clients cannot access the information in Active Directory, you can provision the command lines using a Group Policy with the `ConfigMgrInstallation.adm` template. The template is found on the Configuration Manager 2012 installation media in `.SMSSetup\TOOLS\ConfigMgrADMTemplates`.

Manually Installing the Client

This installation method might sound like a very time-consuming method; however, you will find yourself installing clients manually for several reasons. You can manually install the client by running `CCMSetup.exe` from the site server or from any management point. The file is located in the `Program Files\Microsoft Configuration Manager\Client` folder.

To manually install a client in an environment where the AD schema has been extended, do the following: From Start ➢ Run, type **\\ConfigMgr Server\SMS_<*sitecode*>\Client\ccmsetup.exe**.

To manually install a client on a workgroup computer, follow these steps:

1. Make sure you can access the client installation files or copy them to the local client.
2. Open a command prompt as administrator.
3. Run **ccmsetup.exe smssitecode=PS1 /Source:C:\CM2012Client smsmp=SCCM4.SCCMLAB.Local fsp=SCCM4.SCCMLAB.Local DNSSUFIX=SCCMLAB.Local**.

This will install the Configuration Manager client from the local source `C:\CM2012Client` and assign it to primary site PS1 using SCCM4 as the management point and fallback status point. The client must be able to resolve the site system names; otherwise the installation will fail. You can use the Hosts and LMHOSTS files to provide the needed naming resolution support.

To support a DMZ installation where the client is not able to resolve the needed hostnames, you configure these settings in the LMHOSTS and Hosts files (in the example the site server is named SCCM4.SCCMLAB.LOCAL with 192.168.1.2 as the IP address). You can find the files in `%windir%\System32\drivers\etc\`. There must be exactly 15 characters between the first " and the \ in the LMHOSTS file.

Add these entries to the LMHOSTS file:

```
192.168.1.2 SCCM4 #PRE
192.168.1.2 "SMS_MP         \0x1A" #PRE
```

Add this entry to the Hosts file:

```
192.168.1.2 SCCM4.SCCMLAB.local
```

Client Push

Client push is one of the most used installation methods because it requires very little work. All you need to do is to specify one or more client push installation accounts along with some client push installation settings. Before you use client push, you need to understand the preinstallation phase:

- When one of the discovery processes is running, a client configuration request (CCR record) will be generated for each object that does not have a client installed.
- Using the client push account, the Client Configuration Manager (CCM) component will make a connection to the client and copy the two files `ccmsetup.exe` and `mobileclient.tcf` to `\\Client\Admin$\CCMSetup`.
- Once the files have been successfully copied to the client, the server will verify that the `CCMsetup` service is starting successfully on the client before it disconnects.
- From this point on, the local client is responsible for installing the Configuration Manager agent.

Note: The client push installation feature of Configuration Manager 2012 does not support client installation on Linux/Unix or Mac computers. The client for these platforms must be installed manually or via a remote scripting solution.

All this information from the preinstallation phase is recorded in the `CCM.log` file on the site server. It is not uncommon to see errors in the log file for reasons like these:

- A local firewall is running on the client and no firewall rules have been created. This will generate an error message like this: `---> Failed to connect to \\Client\admin$ using machine account (67)`.
- The client push account does not have the correct permissions to access IPC$ and Admin$. This will generate an error message like this: `Unable to connect to remote registry for machine name "client ", error 5`.

- The client is not running. This will generate an error message like this: `---> Failed to connect to \\Client\admin$ using machine account (67).`
- Configuration Manager is unable to locate the client because of naming resolution errors. This will generate an error message like this: `The network path was not found (53).`

If the client Configuration Manager component fails to start the installation on the client, it will retry the installation once an hour for seven days. All retry attempts are stored in `\Program Files\Microsoft Configuration Manager\inboxes\ccrretry.box`.

To configure the client firewall correctly you need to enable

- File and Printer Sharing
- Windows Management Instrumentation (WMI)

To configure the client push installation account correctly you need to assign it local administrative permissions on the client.

When you create the account, make sure you add it to the group within your Active Directory structure that has the proper security rights on each machine within the site. Once the account(s) are created, you can configure them as client push installation accounts in the Configuration Manager console. If none of the specified client push accounts are able to connect to the client, the site server will attempt to connect using the site server computer account. With that in mind, you can also assign the correct permissions to the site server computer account, thus eliminating the need for multiple client push accounts.

Configuring Client Push Settings

Once the discovery methods have been configured, you will need to configure the client push settings. In the Configuration Manager Administrator console, follow these steps:

1. Select the Administration workspace.
2. Browse to Overview ➢ Site Configuration ➢ Sites.
3. Choose Client Installation Settings ➢ Client Push Installation on the ribbon.

Selecting the check box Enable Automatic Site-Wide Client Push Installation means that whenever a computer is discovered within a defined site boundary group, the client will be automatically installed.

Figure 6.16 shows the Client Push Installation Properties, and this is where you can enable and configure automatic client push installation. It is important to know that client push can be performed in several ways. Use the General tab to configure the options for the fully automated client push feature of Configuration Manager. For a collection-based or client-based client push, you only need to configure settings on the Accounts and Installation Properties tabs.

The Accounts tab, shown in Figure 6.17, allows you to specify the accounts to use to install the Configuration Manager client. Configuration Manager will try the accounts in order until it finds an account with administrative rights on the destination computer. It will always try using the site server's computer account last if one or more accounts are listed and try the site server's computer account only if no accounts are listed. In the figure you will notice that two different accounts, a domain account and a local account, have been specified. A maximum of 10 user accounts can be specified here.

Figure 6.16
The General tab of Client Push Installation Properties

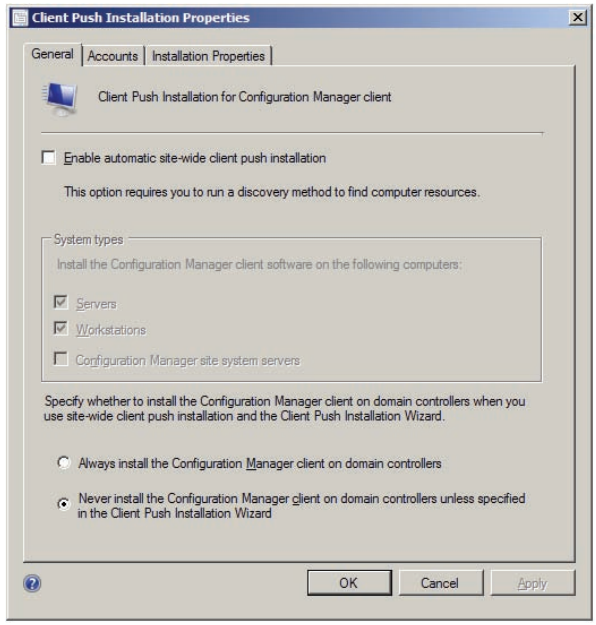
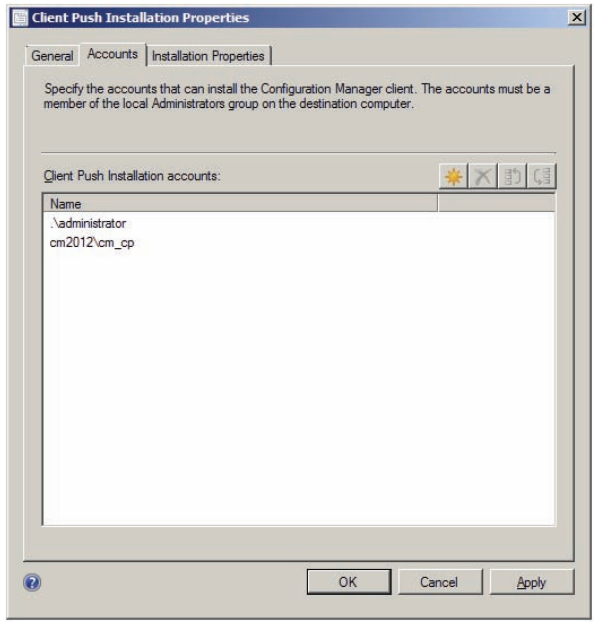


Figure 6.17
The Accounts tab of Client Push Installation Properties



In the Installation Properties tab of Client Push Installation Properties, shown in Figure 6.18, you control how the client is installed by entering installation properties within the text box. The properties that you enter here will be published as command lines in Active Directory. You can enter all available `client.msi` command lines.

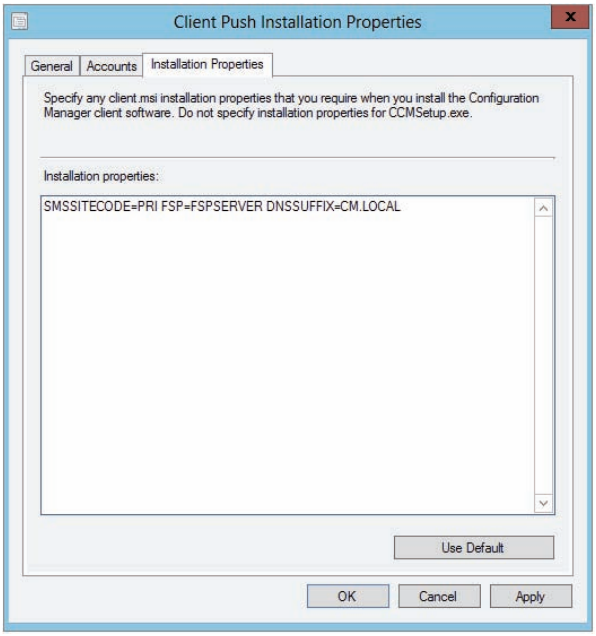


FIGURE 6.18
The Installation Properties tab of Client Push Installation Properties

In order to manually push the client install out from within the Configuration Manager administrative console, the target client system(s) needs to be discovered and visible in the Assets and Compliance workspace. Once a system is available, you can push the client to the individual system, or you can push the client to all of the systems within the collection. The simplest way to do this is with the Install Configuration Manager Client Wizard. To initiate the wizard, select a discovered system or collection and choose Install Client from the ribbon. This will open the Install Configuration Manager Client Wizard.

Although the properties and the installation account cannot be modified from the wizard, as Figure 6.19 shows, you can change some of the client push installation options on an individual basis. Especially notice that you can select which site you want to use to install the client. The site choice also affects from which server the client will download the needed software.

From this page you can also choose to always install the client software. This will force the installation of the client, even if another client is already installed.

You can use the canned reports in the Client Push category to monitor the client push attempts. The reports will provide you with information about all client push attempts divided into days and installation status.

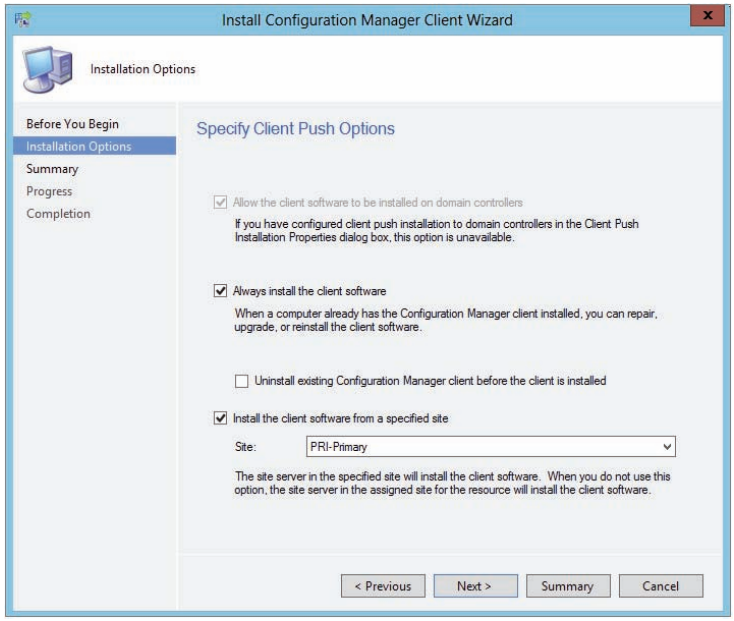


Figure 6.19
Client push Install Configuration Manager Client Wizard settings

Group Policy

You can use a software installation GPO to install the client. For GPO installations you must use the `ccmsetup.msi` file. This file can be found in the folder `.\Program Files\Microsoft Configuration Manager\bin\i386` on the site server. You cannot specify any command-line properties when publishing the client; instead the command lines that are published to Active Directory will be used. If you are installing the client in another forest, you can use a Group Policy based on the `ConfigMgrInstallation.adm` template to provision the command lines locally on the client in the registry before installing the client.

Software Update

This installation method requires that you have an existing WSUS server in the environment and that it is also configured as the software update point. (A Windows client can only be configured with a single WSUS server. For that reason you need to make sure that the WSUS server specified in the GPO is the same as the one being used as the software update point.) Once you enable this method, the Configuration Manager client will be published to WSUS as a required infrastructure update. You cannot specify any command-line properties when publishing the client; instead the command lines that are published to Active Directory will be used. If you are installing the client in another forest, you can use a Group Policy based on the `ConfigMgrInstallation.adm` template to provision the command lines in the registry before installing the client. You can monitor publishing between the site server and WSUS server by reading the `wcm.log` file on the site server.

Note that if you ever need to uninstall Configuration Manager for any reason, make sure you have disabled this client installation method. Failure to do so will leave the Configuration Manager client in WSUS as a required infrastructure update.

Software Distribution

You can deploy the client using the Software Deployment feature. This method is often used when upgrading the client to a new service pack. You will notice that a new installation of Configuration Manager ships with a Configuration Manager client package and a Configuration Manager client Upgrade package. If you want to create your own Configuration Manager client software package, follow these steps:

1. Open the Configuration Manager console and navigate to the Software Library workspace.
2. Select Overview ➢ Application Management ➢ Packages and click Create Package From Definition on the ribbon.
3. Under Name, select Configuration Manager Client Upgrade and click Next.

   If you do not see the definition, verify that you have selected Microsoft as the publisher.
4. Select Always Obtain Files From A Source Directory and click Next.
5. In the source directory type **\\<Server>\sms_<Sitecode>\Client** where `<Server>` is the name of the Configuration Manager site server and `<sitecode>` is the site code.
6. Click Next and finish the guide.

You have now created a software package containing the client software that you can deploy using the deployment methods described in later chapters.

Logon Script Installation

Logon scripts have been used by companies for many years to apply settings to users and their systems. The parameters that you can use are the same as those described earlier in this chapter. When installing the client using this method, remember to add the `/Logon` command line to `ccmsetup.exe`; otherwise, the client installation will begin every time the user logs on to a system.

Imaging

If you are using the Operating System Deployment feature of Configuration Manager, there is a step in the task sequence that will install the Configuration Manager client. The task sequence step Set Up Windows And ConfigMgr is required and will install the Configuration Manager client correctly in both the reference image and the real image. If you are using another imaging solution and need the Configuration Manager client installed in the reference image, follow these steps:

1. Manually install the client.
2. Stop the SMS Agent Host service by running **NET STOP CCMEXEC**.
3. Remove the trusted root key and any other unique certificates. Remove the trusted root key by running **CCMSetup RESETKEYINFORMATION = TRUE**.
4. Run **SYSPREP.EXE**.
5. Capture the image.

Installing Linux/Unix Clients

Beginning with Configuration Manager 2012 SP1, Configuration Manager supports Linux and Unix computers as Configuration Manager clients. The Linux/Unix Configuration Manager client supports hardware and software inventory as well as software distribution. The client push feature of Configuration Manager 2012 cannot be used to install the client, and these computers are treated as workgroup-based devices. As a result, you must manually install the Configuration Manager client on Linux/Unix devices, or you can use a shell script that installs the client remotely.

The client installation process leverages a script named Install, which is included in the downloaded media for the Linux/Unix client. This installation media is available at `www.microsoft.com/en-us/download/details.aspx?id=39360`.

The Install script supports command-line properties, some of which are required and others are optional. For example, you must specify the management point for the site that the Linux/Unix client will utilize. Once the client is installed, you can use the Client Settings feature in the Configuration Manager 2012 console to configure the client agent as you would for Windows-based clients.

You must use the correct client installation package for the Linux/Unix computer that the Configuration Manager 2012 client will be installed on. Several versions of Linux/Unix can utilize the Universal Agent, while other versions will utilize a client installation package that is specific to each operating system version and platform. Use the TechNet article "Supported Distributions of Linux and UNIX" to determine which installation package to use:

```
http://technet.microsoft.com/en-us/library/gg682077.aspx#BKMK_
SupConfigLnUClientReq
```

You can utilize the same installation process and command-line properties, regardless of which installation package is used. Also, the client installation package contains all of the files required to completely install the Configuration Manager 2012 client, and the computer will not download additional files from the management point or another source location during the install process.

As shown in Figure 6.20, the client installation command line will reference the Install script that is included with the client installation package and will also specify the management point, the assigned site, any optional installation configurations, and the client installation package file.

To install the client on a Linux/Unix computer, follow these steps:

1. Copy the Install script file and the client installation `.TAR` file to a folder on the Linux/Unix computer.
2. Use root credentials to run the command to enable the Install script to run: `chmod +x install`.
3. Under the root credentials, run the command with the required parameters and optional items, if needed:

   ```
   ./install -mp <management point> -sitecode <sitecode> <property #1>
   <property #2> <client installation package>
   ```

4. Once the client installation is complete, you can validate the status of the installation via the log file `/var/opt/microsoft/scxcm.log`. You can also verify that the computer registered with Configuration Manager properly by viewing the Devices node in the Assets and Compliance workspace in the Configuration Manager 2012 console.

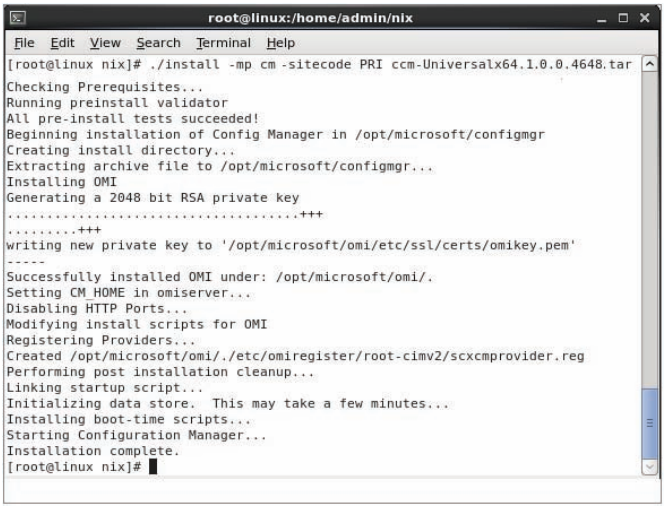


FIGURE 6.20 Linux/Unix client installation

If optional command-line properties are needed during the install, they must be specified in the command before the statement that identifies the client installation package file that will be used. Also, the client installation package file must be specified last in the command line. Table 6.1 describes the available command-line options. You can utilize the property `-h` to display this list of properties that are available.

TABLE 6.1: Available command-line options

PROPERTY	REQUIRED OR OPTIONAL	COMMENTS
`-mp`	Required	This is the FQDN of the management point server that the client will use for initial contact, but it does not specify the management point that the client will use after being assigned to a site. If the management point is configured to accept only HTTPS connections, you must also use the `-UsePKICert` property.
`-sitecode`	Required	This specifies the Configuration Manager primary site server that the client will be assigned to.
`-fsp`	Optional	This is the FQDN of the fallback status point server that the client will utilize to submit state messages.
`-dir`	Optional	This provides an alternate location for the client installation package. The default location is `/opt/microsoft`.

Property	Required or Optional	Comments
-nostart	Optional	This prevents the automatic start of the Configuration Manager client service after the client installation process is completed. After the client install process is complete, you must manually start the client service. The default option is to start the service after the client installation process is complete.
-clean	Optional	This is used to remove all client files and data from a previously installed client before the new installation starts.
-keepdb	Optional	This specifies that the local client database should be retained and reused when the client is reinstalled. The default option is to delete the database when the client is reinstalled.
-UsePKICert	Optional	This specifies the full path and filename for the PKI certificate in the Public Key Certificate Standard format. Use the -certpw command-line parameter to provide the password associated with the PKCS#12 file. If the certificate is not valid or cannot be located, the client will use HTTP and use a self-signed certificate. Also, you must use this property if you use the -mp option to specify a management point that is configured to accept only HTTPS client connections.
-certpw	Optional	This specifies the password associated with the PKCS#12 file that was specified with the -UsePKICert property.
-NoCRLCheck	Optional	This specifies that the client should not check the certificate revocation list when it communicates over HTTPS. The default is that the client will check with the CRL before establishing an HTTPS connection.
-rootkeypath	Optional	This specifies the path and filename for the trusted root key.
-httpport	Optional	This specifies the port that the client uses to communicate with the management point via HTTP. The default value is 80. Note: After installing the client, you cannot change the port configuration. To change the port you will need to reinstall the client and specify the port to utilize. Use the -keepdb option to retain the client database and files.

TABLE 6.1: Available command-line options *(CONTINUED)*

PROPERTY	REQUIRED OR OPTIONAL	COMMENTS
`-httpsport`	Optional	This specifies the port that the client uses to communicate with the management point via HTTPS. The default value is 443. Note: After installing the client, you cannot change the port configuration. To change the port you will need to reinstall the client and specify the port to utilize. Use the `-keepdb` option to retain the client database and files.
`-ignoreSHA256validation`	Optional	This specifies that the client installation will skip SHA-256 validation. Use this option if you're installing a client on an operating system that does not support SHA-256.
`-signcertpath`	Optional	This specifies the full path and filename for the exported self-signed certificate of the site server.
`-rootcerts`	Optional	This allows you to specify additional root certificates that the client may need to validate site servers.

Installing a Mac Client

Configuration Manager 2012 also supports the management of Apple Mac computers as clients. The client for the Mac operating system allows you to discover, retrieve inventory, manage settings, and also deploy applications and security updates via Configuration Manager.

The management of Mac computers in Configuration Manager 2012 requires the use of public key infrastructure (PKI) certificates. Configuration Manager can utilize Microsoft Certificate Services with an enterprise certification authority (CA), or you can request and install computer certificates outside of Configuration Manager as long as the certificate meets the requirements of Configuration Manager. It is worth noting that Mac-based Configuration Manager clients always perform certificate revocation checking and cannot be disabled. If Mac clients cannot confirm the certificate revocation status via the certificate revocation list (CRL), they will not be able to connect to the Configuration Manager site servers. Mac devices will also require that the Configuration Manager enrollment point and enrollment proxy point site system roles are installed and configured.

Mac computers are automatically assigned to the Configuration Manager site that will manage them and are installed as Internet-only clients, even if the Mac computer will communicate only on an internal or intranet network. Thus, you will need to ensure that the site systems in the assigned Configuration Manager site are configured to allow client connections from the Internet.

The following is the process for installing the Configuration Manager client on a Mac computer:

1. Ensure that the proper certificates have been prepared and deployed. A web server certificate must be deployed to the management point, distribution points, the enrollment point, and the enrollment proxy point. Also, a client authentication certificate must be deployed to the management point and distribution point. If you need guidance on preparing a Configuration Manager site for supporting PKI and Internet-based clients, refer to the definitive article "Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority" at `http://technet.microsoft.com/en-us/library/gg682023.aspx`.
2. Open the Configuration Manager 2012 console and select the Administration workspace.
3. In the Administration workspace, choose Client Settings and then select Default Client Settings. You must modify the default client settings in order to configure the enrollment process. These settings cannot be applied via a custom device settings group.
4. Right-click Default Client Settings and select Properties.
5. Select Enrollment and set Allow Users To Enroll Mobile Devices And Mac Computers to Yes.
6. Select Enrollment Profile and click Set Profile.
7. In the Mobile Device Enrollment Profile window, click Create.
8. In the Create Enrollment Profile window, enter a name for the enrollment profile and configure the site code for the Configuration Manager site that will manage the Mac computers.
9. Click Add and in the Add Certification Authority For Mobile Devices window select the certification authority that will issue certificates to Mac computers. Click OK.
10. In the Create Enrollment Profile window, select the Mac computer certificate template that was previously created and click OK.
11. Click OK to close the Enrollment Profile window, and click OK to apply the settings to the default client settings.
12. Download the Mac installation media client files and install the Mac client. The Mac client applications are contained in a file named `ConfigmgrMacClient.msi` and can be obtained at `http://www.microsoft.com/en-us/download/details.aspx?id=36212`.
13. On a Windows computer, run the `ConfigmgrMacClient.msi` file and extract the files that are included in the MSI.
14. Copy the `Macclient.dmg` file from the extracted files to the Mac computer.
15. Run the `Macclient.dmg` file on the Mac computer to extract the Mac client installation files. This will create a `Tools` folder and will contain several Mac client tools and files, including ccmsetup and `cmclient.pkg`.
16. For Configuration Manager 2012 R2 you have two options for enrolling the Mac client. You can use the CMEnroll tool that is included in the extracted media from the previous step, or you can use the Mac Computer Enrollment Wizard.

Here are the steps for the CMEnroll process:

a. To use the CMEnroll process, open the folder where the extracted files were stored and enter the following command line: **`Sudo ./ccmsetup`**. Wait for the Completed installation message to appear. Do not restart the computer.

b. Open the folder where the extracted files were stored and enter the following command line: **`Sudo ./CMEnroll -s <enrollment proxy server> -ignorecertchainvalidation -u <user name>`**. The user name must match an active account in Active Directory that has been granted Read and Enroll permissions on the Mac client certificate template. Also, this command will prompt for the password for the super user account first and then prompt for the password for the Active Directory user account. Make sure you use the correct passwords.

c. Wait for the message stating that the Mac client has been successfully enrolled, and then restart the computer.

Here are the steps for the Mac Computer Enrollment Wizard process:

a. To use the Mac Computer Enrollment Wizard, click Next at the welcome page. The Mac Computer Enrollment Wizard is shown in Figure 6.21.



FIGURE 6.21
Mac Computer Enrollment Wizard

b. Enter the required information. The user name can be in domain\username format or username@domain.

c. The user name and the password must match an Active Directory account that has been granted Read and Enroll permissions on the Mac client certificate template.

d. Enter the password that is associated with the specified user account.

e. For server name, enter the name of the enrollment proxy point server.

f. Click Next and complete the wizard.

Once the client installation is complete, you can verify that the Mac computer registered properly by viewing the Devices node in the Assets and Compliance workspace in the Configuration Manager 2012 console.

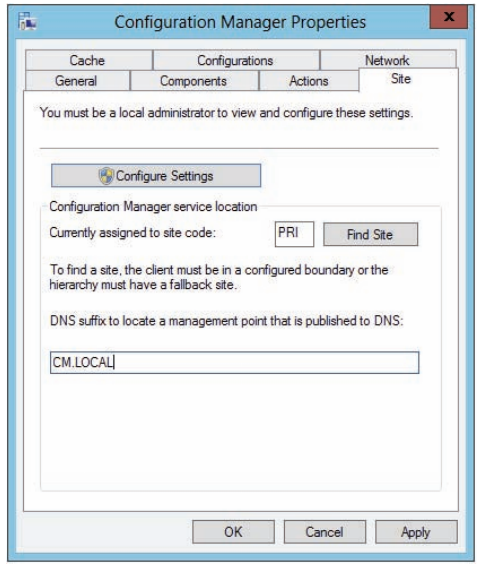
Verifying Client Installation

While the installation is in progress, you can view the installation program running within Task Manager or monitor the installation by reading the log files. In Task Manager you will see `ccmsetup.exe` running. As it completes, you will see `ccmsetup.exe` replaced by the agent host program `ccmexec.exe`.

You can also verify that the client has obtained the correct site code and is communicating with the management point, as follows:

1. Open Control Panel, and you will find a new icon named Configuration Manager.
2. Double-click this icon, and the Configuration Manager Properties screen will appear.
3. Click the Site tab to find the site code within the Currently Assigned To Site Code box, as shown in Figure 6.22.

FIGURE 6.22
Verifying that the site code has been obtained



Within the Actions tab of the Configuration Manager Properties screen, you should also find several actions listed by default; other actions will appear in this list as the client agents are enabled. The default actions are Application Deployment Evaluation Cycle, Discovery Data Collection Cycle, Hardware Inventory Cycle, Machine Policy Retrieval & Evaluation Cycle, User Policy Retrieval & Evaluation Cycle, and Windows Installer Source List Update Cycle. Each of these actions will be covered when we discuss the related components.

Now, unless you have a very small environment, you will not be able to manually verify the installation of each client. Instead you will use the following reports in the Site - Client Information category:

- Client Deployment Success Report
- Client Deployment Status Details
- Client Assignment Status Details
- Client Assignment Success Details

The reports require that you have specified a fallback status point in the command line for the client installation.

Troubleshooting a Client Installation

To troubleshoot a client installation you will need to understand the three phases in the process. You can troubleshoot each of the phases in real time by reading the correct log files with `CMtrace.exe`.

The Preinstallation Phase This phase is described in the "Client Push" section of this chapter. A useful log file in this phase is `ccm.log` on the site server.

The Installation Phase This phase begins when `ccmsetup.exe` reads the `mobileclient.tcf` file and starts downloading the required files needed to complete the installation. Useful log files in this phase are `ccmsetup.log` and `client.msi.log`, both found in the `%windir%\ccmsetup` folder on the client.

The Post-installation Phase This phase is also known as the assignment phase, where the client is being added as a managed client to a primary site. Useful log files in this phase are `clientidstartupmanager.log`, `clientlocation.log`, and `locationservices.log`, all found in the `%windir%\ccm\logs` folder on the client.

Once you have identified where the problem is, you will be able to select the correct log file for further troubleshooting.

Ensuring Client Health

Client status and automatic client remediation are some of the new features in Configuration Manager 2012. In previous versions of Configuration Manager/Systems Management Server, organizations were forced to spend numerous hours creating custom client health solutions, and even more organizations did not even implement a client health process. In Configuration Manager an automatic remediation process runs daily on every client, and reports and alerts tell you if the number of active clients is dropping to a number below the defined service-level agreements for the company.

Automatic Client Remediation

During the client installation a schedule remediation task is created in Windows. Figure 6.23 shows the scheduled task in Task Scheduler. The process `ccmeval` will run daily and perform

all the checks that are specified in the `ccmeval.xml` file found in the `%windir%\ccm` folder. There are more than 20 different checks. If the evaluation process fails, the client will automatically be repaired. All `ccmeval` status messages will be forwarded to the management point. You can monitor the process by reading the `ccmeval.log` and `CcmEvalTask.log` files found in `%windir%\ccm\logs` and the `ccmsetup-ccmeval.log` file found in `%windir%\ccmsetup\`.

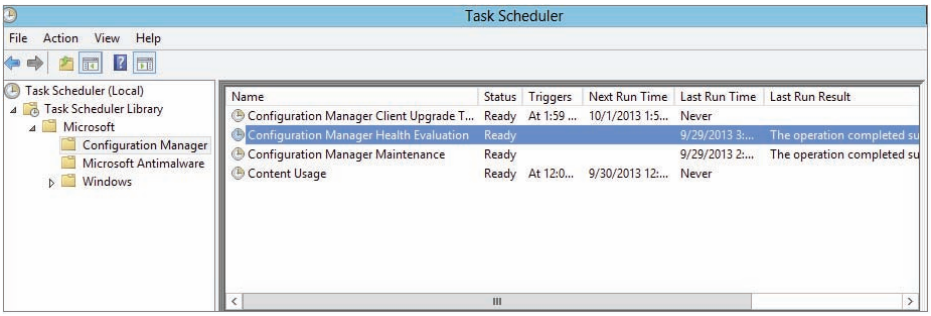


FIGURE 6.23
CCM evaluation task

You can monitor the client remediation process in the Configuration Manager console. Navigate to the Monitoring workspace and select Client Status ➢ Client Check.

Determining Client Health

To determine the overall client health Configuration Manager uses multiple objects such as these:

- Discover records
- Hardware inventory
- Software inventory
- Status messages
- Policy requests
- Active Directory integration

As the administrator, you will define when a client goes from being considered active to inactive. To configure the client activity settings, follow these steps:

1. Navigate to the Monitoring workspace.
2. Select Client Status.
3. From the ribbon click Client Status Settings to open the window shown in Figure 6.24.

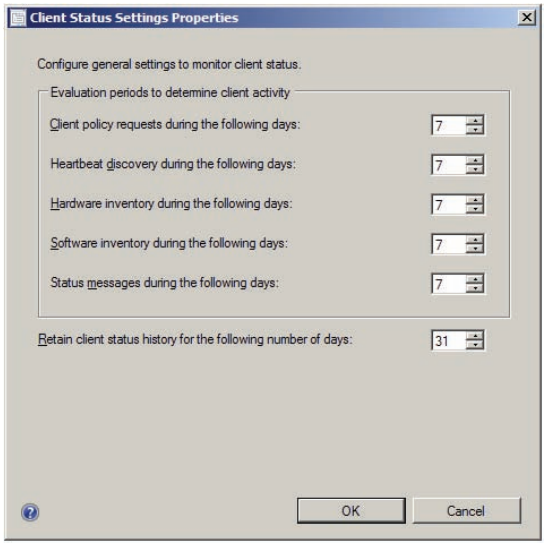


FIGURE 6.24
Client Status Settings Properties—General tab

There are no correct or incorrect settings; it all depends on the client behavior in your network. Do you have only workstations that are supposed to be started daily, or do you have a large number of laptops that are infrequently connected to the network? Don't be too aggressive when configuring the settings. If you configure the wrong values, you might find yourself chasing ghosts and trying to troubleshoot clients that for obvious reasons are not connected to the network.

Monitoring Client Status

The client status data is displayed in the Monitoring workspace. When you click the Client Status node, you will see both the client activity and the client check data. If you click any of the different states, you will be taken to the Assets and Compliance workspace, where you will see all the devices that are in the selected state.

You can also use the canned reports in the Client Status category. They will provide you with valuable information about the overall health status and the client agility.

Client Status Summary Can be used as the main client health report. It will give an overview of the client health and client activity data.

Inactive Client Details Will list all inactive clients along with information about the last health check.

Client Status History Will provide a very good historic view for the last 30–90 days.

Client Time To Request Policy Will display how many clients have requested policies during the last 30 days.

Configuring Alerts

Having a mixed environment with laptops, desktops, and servers often means that you have different activity requirements. You can configure individual thresholds per collection and that way have different settings for the unique computer roles in your environment. Figure 6.25

shows the alerts settings that are configured for a collection containing all servers. Because you can use Configuration Manager to keep the servers compliant with software updates, it is unacceptable to have a server running without a healthy client.

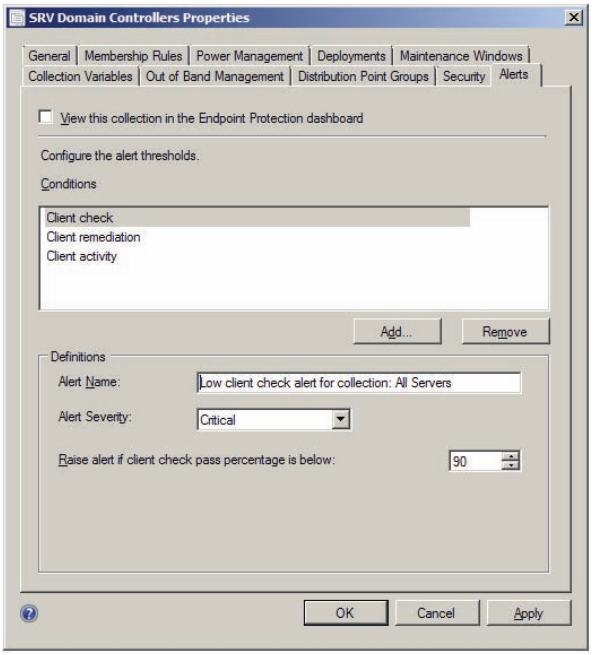


Figure 6.25
Configuring alert settings on a collection

Configuring Client Health Alerts for the All Servers Collection

As the Configuration Manager administrator, you have been requested to ensure that alerts are generated if any servers become unhealthy. To do so, follow these steps:

1. Open the Configuration Manager 2012 administrative console.
2. Select the Assets and Compliance workspace, and browse to Device Collections.
3. Select your All Servers collection, and click Properties on the ribbon.
4. Select the Alerts tab, click Add, and select each of the three Client Status checks.
5. Click OK.
6. In Conditions select each of the Client Status checks and configure the threshold and alert severity.
7. Click OK to save the settings.

To monitor the alerts, do the following:

1. Navigate to the Monitoring workspace.
2. Select Alerts.
3. In the Search field, type **Client** and click Search.

You will now see a list of all client remediation, client health, and client activity alerts.

Automatic Client Upgrade

Configuration Manager 2012 provides the ability to automatically upgrade the Configuration Manager client software on Windows-based devices to the latest version when the site determines that the Configuration Manager client version that is being used is lower than the version that is being used in the hierarchy. The configuration options are shown in Figure 6.26.

Configuration Manager 2012 automatically creates a client upgrade package and deploys the content to all of the distribution points in the hierarchy (except for cloud-based distribution points). As changes are made to the client package, for example, adding a client language pack, Configuration Manager 2012 will automatically update the package and update the distribution points. If automatic client upgrade is enabled, all clients will install the new client language pack automatically. The automatic upgrade feature was originally intended for upgrading relatively small numbers of Configuration Manager 2012 clients, but with the performance improvements in SP1 and R2 it is possible that the automatic client upgrade feature is the primary method you will use for upgrading clients. As always, you should test heavily in your environment and verify that this feature will not cause unexpected performance or network issues.

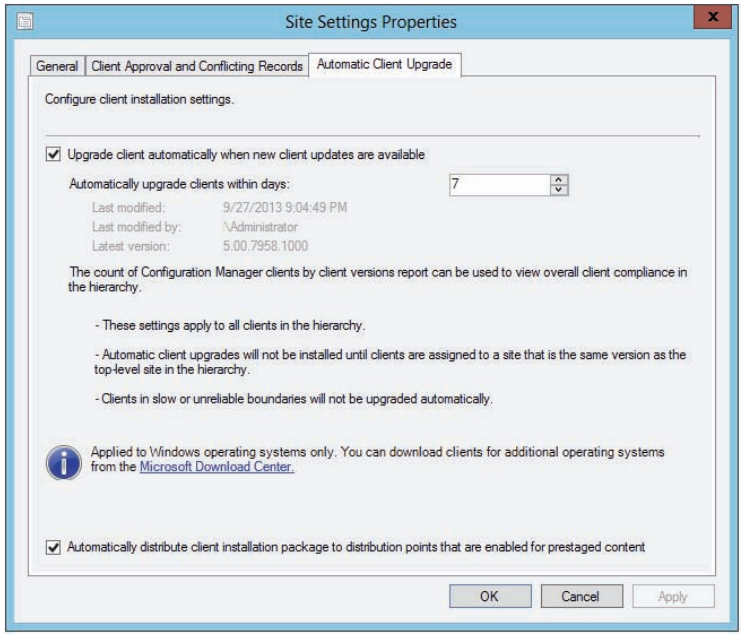


FIGURE 6.26
Automatic Client Upgrade configuration

The following is the process to configure the automatic client upgrade feature:

1. Open the Configuration Manager 2012 console and select the Administration workspace.
2. Select Site Configuration and then select Sites.
3. In the Home tab of the ribbon, click Hierarchy Settings.
4. In the Site Settings Properties window, select the Automatic Client Upgrade tab.
5. If you want to enable the automatic client upgrade feature, select the check box.
6. A window will appear confirming that you have chosen to enable automatic upgrade of all clients in the hierarchy and reminding you that all clients in the hierarchy will be upgraded. Click OK.
7. Configure the number of days in which the client computers must upgrade the client software. The clients will be upgraded at a random interval over the specified number of days. This will help prevent performing a large number of client upgrades at the same time.
8. The option Automatically Distribute Client Installation Package To Distribution Points That Are Enabled For Prestaged Content should be enabled if you want the client installation package to be copied to distribution points that are enabled for prestaged content.
9. Once the settings are configured, click OK to save the settings and close the Site Settings Properties window. Clients will receive the updated setting during their next policy polling check.

The Bottom Line

Configure boundaries and boundary groups. Before starting any client installation, verify that you have configured a boundary group for site assignment.

> **Master It** Let Configuration Manager Forest Discovery automatically create the boundaries and add them to the correct boundary groups.

Select the relevant discovery methods. You configure discovery methods in the Configuration Manager console. The Active Directory discovery methods all require a schedule and an LDAP path. There are schedules for delta and full discovery. In Configuration Manager 2012, delta discovery will also find changes to existing objects; this eliminates the need to run a full discovery more than once a week.

> **Master It** Always know what you want to discover and where. Based on that knowledge, configure the needed discovery methods.

Employ the correct client installation methods. When configuring the client installation methods, make sure you know the pros and cons for each method. Some require firewall settings; others require local administrative permissions. You need to make sure that all the required settings are in place. Do not start any installation until you have the needed site systems, boundary groups, and command lines specified.

Master It Configure the correct command-line properties and ensure they will work for all environments (local forest, workgroup, and DMZ). Create multiple client push installation accounts, and ensure that you have a good understanding of the three phases (pre-installation, installation, and post-installation).

Manage Unix/Linux and Mac devices. Configuration Manager 2012 provides support for managing Unix/Linux and Mac computers as devices. You are now able to manage your entire computer infrastructure from a single management console.

Master It Understand the installation methods available for deploying the Configuration Manager client to the Unix/Linux computers and Mac computers. Remember that client push cannot be used for these devices.

Ensure client health. Client status might not be the first task you think about when implementing a system like Configuration Manager. But it is crucial to the daily administration that you can trust the numbers you see in the reports and in the console. One way to ensure that is by making certain that all clients are healthy and are providing the server with up-to-date status messages and discovery information.

Master It Discuss the different environments that exist in your organization, and use that information when configuring client health alerts. Make sure that you know the client activity during a normal period and that you have a set of defined SLAs for each of the environments (laptops, road warriors, servers, call center, and so on).



Chapter 7

Client Health

Maintaining healthy Configuration Manager clients is critical for delivering Configuration Manager services and meeting required service-level agreements. When clients in the environment are not healthy, the accuracy and dependability of Configuration Manager services are degraded, resulting in systems that are either completely or partially unmanaged.

Client health has been a challenge historically with Configuration Manager, and many tools or processes have been developed to help identify and repair broken clients. The most recent offering from Microsoft was the Client Status Reporting tool, which arrived in Configuration Manager 2007 R2. While good, many of these tools fall short in that client health problems must be managed manually, and automatic remediation is not generally part of the process. Configuration Manager 2012 R2 changes the game in a dramatic way by not only detecting health problems through a thorough set of diagnostics but automatically remediating the problems as well. Before continuing, we must point out that no solution is 100 percent effective, and there will be problems that can't be resolved automatically. However, the majority of client problems that happen now are anticipated to be those that happen because of external issues not related to Configuration Manager specifically. The inclusion of client health evaluation/remediation by default in Configuration Manager 2012 R2 will significantly enhance the stability of deployments. While this solution won't address every potential issue, it goes a long way to reducing administrator workload in keeping systems active and healthy.

This chapter details the client health mechanism in Configuration Manager 2012 R2.

In this chapter, you will learn to

- Detail client health evaluations in Configuration Manager 2012 R2
- Review client health results in the Configuration Manager console

Understanding the Client Health Mechanism

Managing client health issues involves detecting potential issues and fixing problems as they arise. Configuration Manager clients can become unhealthy for any number of reasons, often because of external issues such as WMI failure, DCOM permissions, service failures, and more. Configuration Manager 2012 introduces an automated mechanism to detect the most common client health issues and automates the process of fixing the problem. While this mechanism will go a long way toward helping maintain healthy clients, there will likely still be situations where manual intervention is required, but those situations should be greatly minimized.

Any tool to effectively validate and potentially repair client health issues, by definition, must be able to execute independently without relying on a healthy client to operate. Further, such a tool must execute locally to mitigate any potential network issues. The client health tool in Configuration Manager 2012 addresses this requirement nicely by running as a scheduled task—set apart from the client itself. The next section reviews the elements of this scheduled task for implementing the client health scanning.

Scheduled Task

The client health tool in Configuration Manager 2012 operates as a scheduled task. The required scheduled task is automatically created when the Configuration Manager 2012 client is installed and set to run daily or a bit past midnight. Figure 7.1 shows the scheduled task created on a client system.

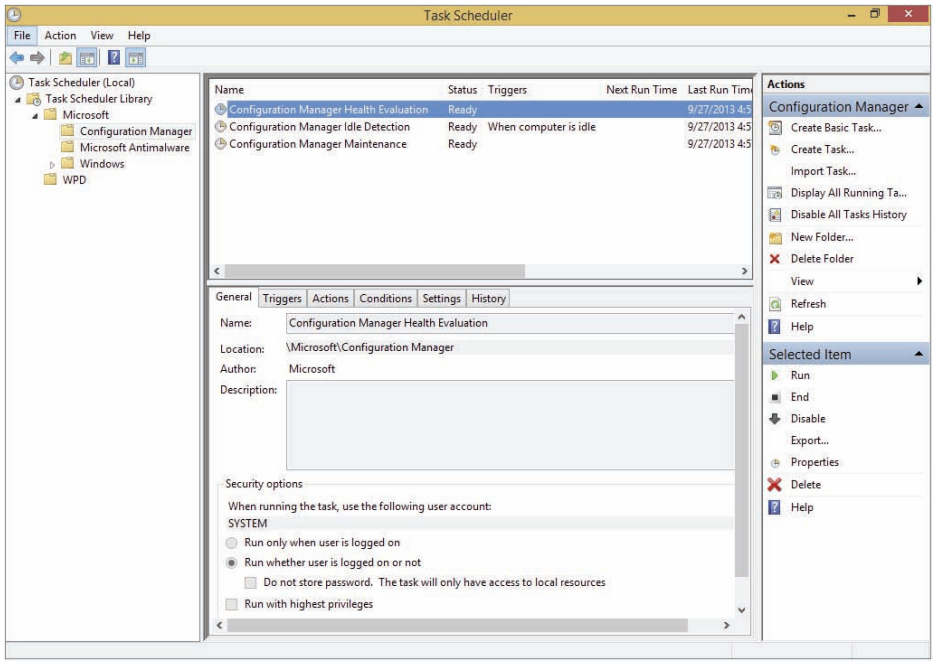


FIGURE 7.1 Scheduled task created by a client installation

DIFFERENCES BETWEEN PLATFORMS

All platforms supported for use with the Configuration Manager client also support the client health scheduled task, but there are differences in the way various configurations may appear between platforms. The example discussion focuses on a Windows 7 workstation.

The overview of the scheduled task shown in Figure 7.1 provides helpful information, including the last run time and next run time for the task and whether the task was successful.

Client Health vs. Problem-Free Execution

A successful task doesn't necessarily mean that the Configuration Manager client is healthy; it simply means that the client evaluation tool was able to execute without encountering a problem.

Notice that this view also provides various tabs that allow you to view the underlying configuration for the scheduled task. In order to make any changes to the task, you must select the properties for the task, which will present the same information but in an editable format, as shown in Figure 7.2 and described in the following sections.

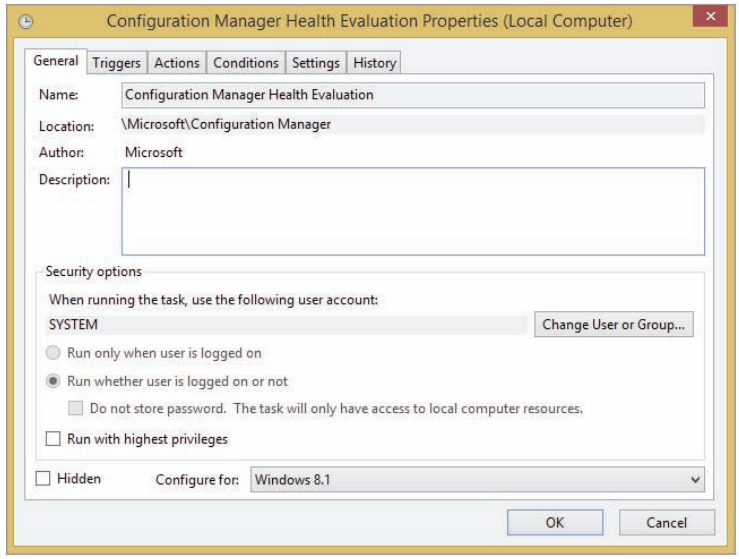


Figure 7.2 Properties window for the scheduled task

Triggers Tab

The Triggers tab of the scheduled task, shown in Figure 7.3, is the place where you might adjust the run schedule for the scheduled task.

Actions Tab

The Actions tab of the scheduled task, shown in Figure 7.4, shows the command line that is to be executed when the scheduled task runs. As you can see from the figure, the task executes `CCMEval.exe`, which is in the `%WINDIR%\CCM` directory. We'll discuss CCMEval in more detail shortly. No command-line parameters are needed for this executable.

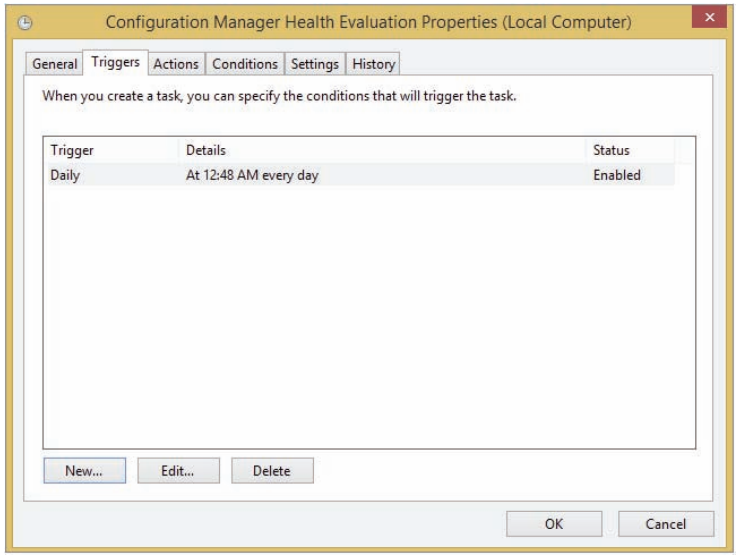


Figure 7.3
Triggers tab for the scheduled task

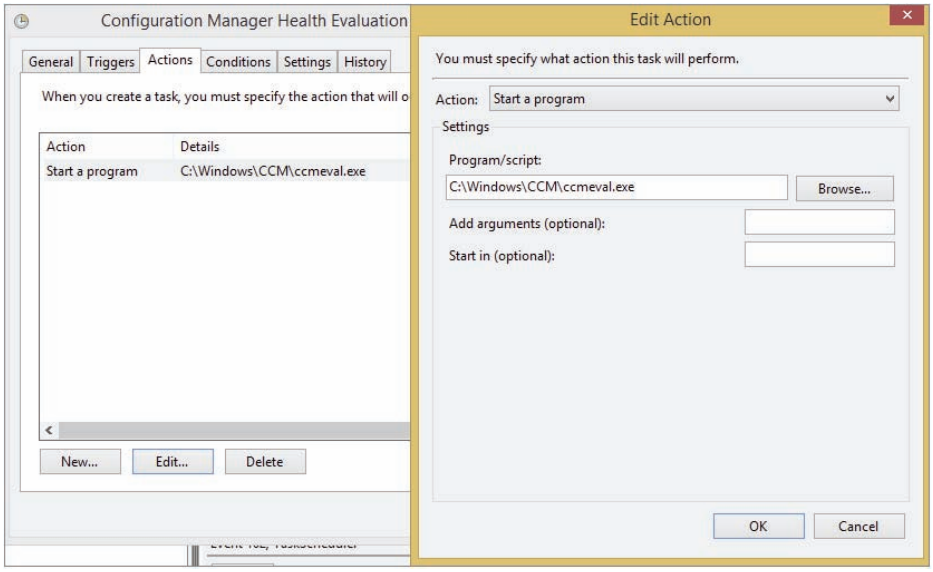
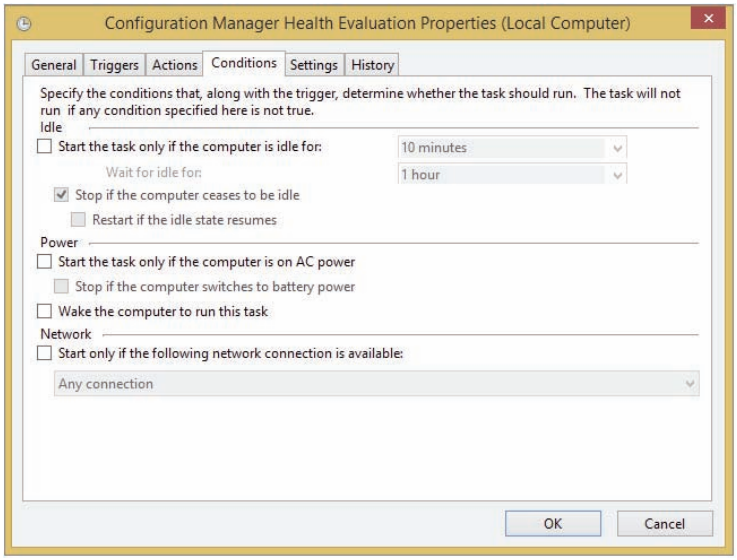


Figure 7.4
Actions tab for the scheduled task

Conditions Tab

The Conditions tab, shown in Figure 7.5, allows administrators to specify specific conditions that must be met before starting the task. There are no conditions set on this tab by default.

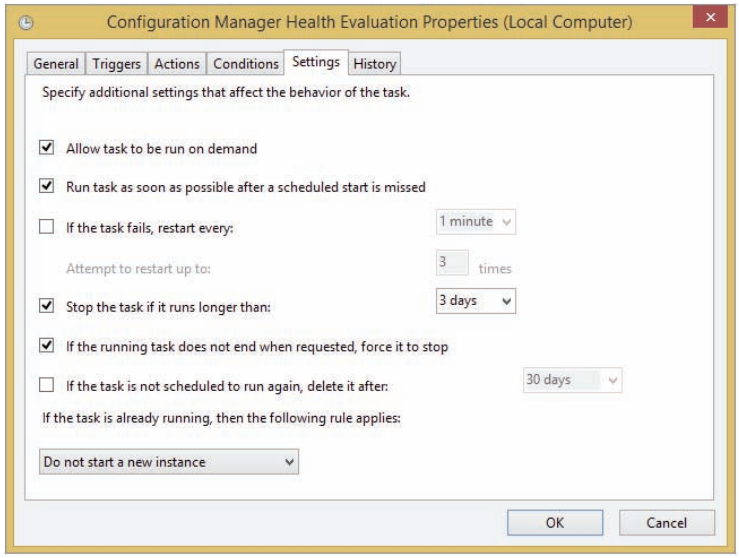
Figure 7.5
Conditions tab for the scheduled task



Settings Tab

The Settings tab, shown in Figure 7.6, specifies various settings for the task. The default values configured are as follows:

Figure 7.6
Settings tab for the scheduled task



Allow Task To Be Run On Demand This setting specifies that the task can be started by administrators as needed, such as in troubleshooting scenarios, outside the scheduled start time.

Run Task As Soon As Possible After A Scheduled Start Is Missed This setting specifies the run behavior for the task if the system isn't able to run it on the defined schedule. As an example, if the system is powered off overnight and cannot run the task at the assigned time, then the task will be initiated the next time the system is started. The CCMEval process is lightweight but in this scenario is just one more thing for a system to do during startup, a process already loaded with significant activity. To avoid additional system load during startup caused by running this task, it may be worth considering rescheduling the start time for the task so that it takes place when the system is anticipated to be available.

Stop The Task If It Runs Longer Than This setting ensures that a hung task doesn't continue to run long term. The default setting for this is 3 days, and it's unlikely that the CCMEval task will run into issues causing the process to hang. Having this set as a failsafe, though, is a good idea.

If The Running Task Does Not End When Requested, Force It To Stop This setting works with the previous setting and will force the CCMEval thread to terminate if it remains in a hung state even after termination is requested.

The last setting, Do Not Start A New Instance, prevents multiple instances of CCMEval from spinning up.

History Tab

The History tab, shown in Figure 7.7, allows administrators to review the execution history for the task. There are no configurable settings on this tab.

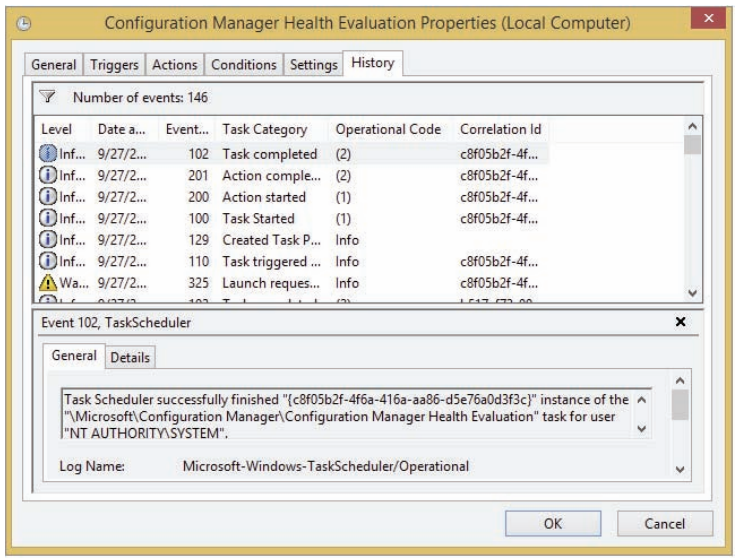


Figure 7.7
History tab for the scheduled task

CCMEval Process

The task to execute CCMEval runs on a daily schedule by default. It is fully possible to change this schedule, but it's not recommended. If needed, the task can be run manually for troubleshooting or other purposes, as previously alluded to.

With the understanding that client health checking and remediation for Configuration Manager 2012 clients is handled by CCMEval, it's natural to wonder what this process actually does. That's the next part of the discussion.

CCMEval is an executable that exists in the `%WINDIR%\CCM` folder on all Configuration Manager 2012 clients, as shown in Figure 7.8.

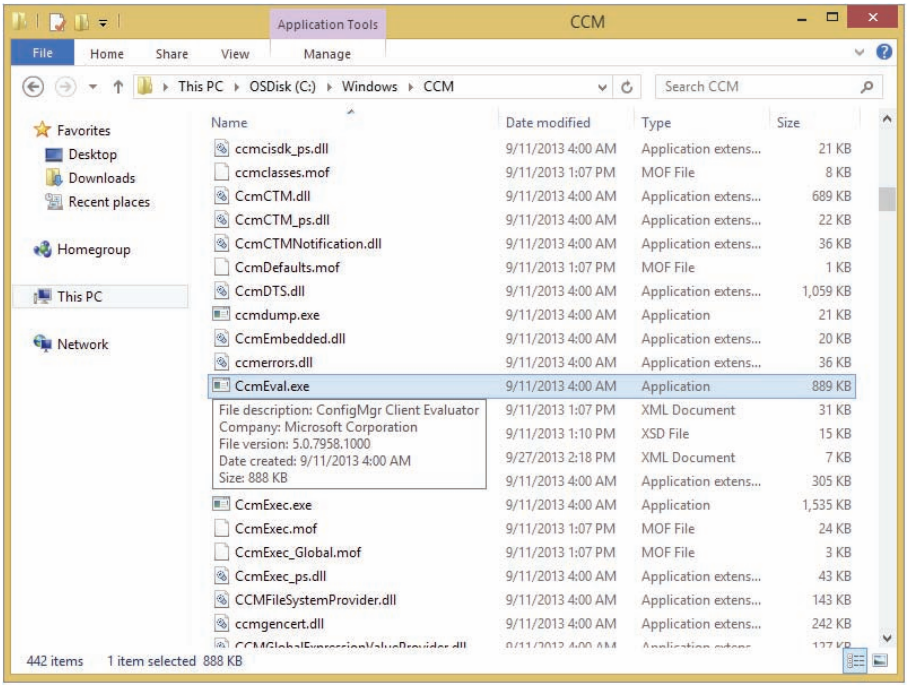


FIGURE 7.8 CCMEval executable in the `%WINDIR%\CCM` folder

Note that in addition to `CCMEval.exe` there are also `CCMEval.xml`, `CCMEval.xsd`, `CCMEvalReports.xml`, and `CCMEval.log`. These are support files for the CCMEval process and are used as follows:

`CCMEval.exe` This is the executable file used to drive the health evaluation and remediation process on Configuration Manager 2012 clients.

`CCMEval.xml` This is the control file that defines the tests and remediation actions that will be taken as a result of test conditions. This file will be discussed in some detail shortly.

`CCMEval.xsd` This file defines the schema used to validate client health evaluation and report data.

CCMEvalReports.xml This is a header file used for building reporting information forwarded to Configuration Manager 2012 servers.

CCMEval.dll This is a library file for use with CCMEval.exe.

CCMEval.log This file records the progress of health check and remediation activities and is located in the Windows\CCM\logs folder.

Understanding the health check and remediation mechanism provided by CCMEval requires reviewing the work that is done during a CCMEval cycle along with the various checks that are performed. You can mine this information by reviewing CCMEval.xml along with CCMEval.log, and it will help you understand what is happening behind the scenes. Table 7.1 lists the checks and potential remediation outcomes that take place when problems are found during evaluation.

TABLE 7.1: CCMEval evaluation tasks and potential remediation actions

Evaluation Task	Potential Remediation Action
Verify WMI service exists.	No remediation.
Verify/remediate WMI service startup type.	Sets the Windows Management Instrumentation service's startup type to automatic.
Verify/remediate WMI service status.	Sets the Windows Management Instrumentation service to a running state.
WMI repository read/write test.	Remediation of this client check is performed only on computers that run Windows Server 2003, Windows XP (X64), or an earlier version.
Verify/remediate client WMI provider.	Restart the Windows Management Instrumentation service. This remediation is performed only on computers that run Windows Server 2003, Windows XP (64 bit), or earlier versions.
WMI repository integrity test.	Checks that ConfigMgr client entries are present in WMI; if not, it will reinstall the ConfigMgr client.
Verify BITS exists.	No remediation.
Verify/remediate BITS startup type.	Sets the BITS service to the expected startup type.
Verify/remediate client prerequisites.	Checks that client prerequisites are installed. Reads the file ccmsetup.xml in the client installation folder to discover the prerequisites. Then it installs the client prerequisites.
Verify/remediate client installation.	Reinstalls the client.
Verify SMS Agent Host service exists.	No remediation.

Evaluation Task	Potential Remediation Action
Verify/remediate SMS Agent Host service startup type.	Sets the client (SMS Agent Host) service startup type to automatic.
Verify/Remediate SMS Agent Host service status.	Starts the SMS Agent Host service.
WMI Event Sink Test.	Checks whether the ConfigMgr-related WMI event sink is lost and then restarts the client service.
Microsoft policy platform WMI integrity test.	Checks the integrity of policy platform WMI data structures.
Verify/remediate Microsoft Policy Platform service existence.	Installs Microsoft Policy Platform.
Verify/remediate Microsoft Policy Platform service startup type.	Resets the service startup type to manual.
Verify/remediate antimalware service startup type.	Resets the services startup type to automatic.
Verify/remediate antimalware service status.	Starts the antimalware service.
Verify/remediate Network Inspection Service start type.	Resets the service startup type to manual.
Verify/remediate Windows Update service startup type.	Resets the startup type to automatic or manual.
Verify/remediate Windows Update service startup type on Windows 8.	Resets the service startup type to manual or automatic (trigger).
Verify/remediate Configuration Manager Remote Control service startup type.	Resets the service startup type to automatic.
Verify/remediate Configuration Manager Remote Control service status.	Starts the Remote Control service.
Verify/remediate Configuration Manager Proxy service startup type.	Resets the ConfigMgr Wakeup Proxy service startup type to automatic; this remediation is performed only if the Power Management: Enable Wakeup Proxy client setting is set to Yes on supported operating systems.
Verify/remediate Configuration Manager Proxy service status.	Starts the ConfigMgr Wakeup Proxy service; this client check is made only if the Power Management: Enable Wakeup Proxy client setting is set to Yes on supported client operating systems.
Verify that the Microsoft SQL CE database is healthy.	Reinstalls the ConfigMgr client.

Figure 7.9 shows a portion of the `CCMEval.xml` file that contains the rules that are used during the client health/remediation evaluation cycle.

Figure 7.10 is an example of the `CCMEval.log` file after an evaluation cycle is complete. Experienced administrators may notice that after the health-checking cycle is complete, the report is sent back to the site in the form of a state message. We mentioned earlier that an effective client health tool must function independently and not rely on a client function for any of its operation. State messages are commonly sent by the Configuration Manager client, so you might question whether the health evaluation tools simply offload the resulting state report to the client or handle it independently. The latter is true; client health forwards the state message directly to the client's management point using its own mechanism. This is also noted in the log snippet in the figure.

FIGURE 7.9
`CCMEval.xml` example

```
<?xml version="1.0"?>
- <ClientHealth Version="1.1" xmlns:ns="http://schemas.microsoft.com/SystemsManagementServer/2008/05/ClientHealth">
  - <HealthCheck Type="Services" ID="4AB7D77D-3BB0-4EAB-BEFD-7C0F7DA10296" Description="Verify WMI service exists.">
      <Applicability ClientVersion="ALL" OS="ALL" Platform="ALL"/>
      <PARAM Description="Services Check" Order="1"> ServiceExists </PARAM>
      <PARAM Description="Service Name" Order="2"> Winmgmt </PARAM>
    </HealthCheck>
  - <HealthCheck Type="Services" ID="518C0699-03F8-4F38-85C4-4D319EAEFC05" Description="Verify/Remediate WMI service
    startup type." DependsOn="4AB7D77D-3BB0-4EAB-BEFD-7C0F7DA10296">
      <Applicability ClientVersion="ALL" OS="ALL" Platform="ALL"/>
      <PARAM Description="Service Check" Order="1"> ServiceStartupType </PARAM>
      <PARAM Description="Service Name" Order="2"> Winmgmt </PARAM>
      <PARAM Description="Expected Service Startup State" Order="3"> Automatic </PARAM>
    - <Remediate>
        <PARAM Description="Services Remediation" Order="1"> ServiceStartupType </PARAM>
        <PARAM Description="Service Name" Order="2"> Winmgmt </PARAM>
        <PARAM Description="Desired Service Startup State" Order="3"> Automatic </PARAM>
      </Remediate>
    </HealthCheck>
  - <HealthCheck Type="Services" ID="7F4B6E15-2221-455B-9615-93C379E470D5" Description="Verify/Remediate WMI service
    status." DependsOn="4AB7D77D-3BB0-4EAB-BEFD-7C0F7DA10296">
      <Applicability ClientVersion="ALL" OS="ALL" Platform="ALL"/>
      <PARAM Description="Service Check" Order="1"> ServiceStatus </PARAM>
      <PARAM Description="Service Name" Order="2"> Winmgmt </PARAM>
      <PARAM Description="Expected Service Status" Order="3"> Active </PARAM>
    - <Remediate>
        <PARAM Description="Services Remediation" Order="1"> ServiceStatus </PARAM>
        <PARAM Description="Service Name" Order="2"> Winmgmt </PARAM>
        <PARAM Description="Desired Service Status" Order="3"> Running </PARAM>
      </Remediate>
    </HealthCheck>
  - <HealthCheck Type="WMI" ID="14E6774A-1795-4E09-B17D-B6F36A124205" Description="WMI Repository Read/Write
    Test.">
      <Applicability ClientVersion="ALL" OS="ALL" Platform="ALL"/>
      <PARAM Description="Repository Rread/Write Test" Order="1"> RepositoryReadWriteTest </PARAM>
    - <PARAM Description="Check Rules XML" Order="2">
        <![CDATA[ <WmiChecks version="1.0"> <WmiCheck feature="General"> <Root type="Namespace" path="root"> <Child
        type="Namespace" path="ccm"> <ValidationAction type="NoExistCreate" order="Pre"></ValidationAction> <Child
        type="Namespace" path="evaltest"> <ValidationAction type="NoExistCreate" order="Pre"></ValidationAction> <Child
```

FIGURE 7.10
`CCMEval.log` sample

```
<![LOG[Evaluating health check rule {9040BA8C-580D-4FCA-8846-BBD5F5BB1597} : Verify/Remediate Configuration Manager Remote Control service
<![LOG[Result: Not Applicable, ResultCode: 0, ResultType: 0, ResultDetail: ]LOG]!><time="15:30:20.025+240" date="10-30-2013" component="Ccm
<![LOG[Evaluating health check rule {9DCD49EF-E021-46FF-A777-49210B558527} : Verify/Remediate Configuration Manager Remote Control service
<![LOG[Result: Not Applicable, ResultCode: 0, ResultType: 0, ResultDetail: ]LOG]!><time="15:30:20.025+240" date="10-30-2013" component="Ccm
<![LOG[Evaluating health check rule {934F12E3-295E-4BA0-AE0F-09859685720F} : Verify/Remediate Configuration Manager Proxy service startup t
<![LOG[Result: Not Applicable, ResultCode: 0, ResultType: 0, ResultDetail: ]LOG]!><time="15:30:20.049+240" date="10-30-2013" component="Ccm
<![LOG[Evaluating health check rule {43029EED-EB9D-4E35-A5F7-7FDD93EC8C57} : Verify/Remediate Configuration Manager Proxy service status.]L
<![LOG[Result: Not Applicable, ResultCode: 0, ResultType: 0, ResultDetail: ]LOG]!><time="15:30:20.067+240" date="10-30-2013" component="Ccm
<![LOG[Evaluating health check rule {7B9F8FF6-EDF7-42CA-A67F-073A2E161C19} : Verify/Remediate SQL CE database is healthy.]LOG]!><time="15:3
<![LOG[Successfully evaluated all client health rules.]LOG]!><time="15:30:20.068+240" date="10-30-2013" component="CcmEval" context="" type
<![LOG[Client is set to use HTTPS when available. The current state is 224.]LOG]!><time="15:30:20.082+240" date="10-30-2013" component="Ccm
<![LOG[MapNLMCostDataToCCMCost() returning Cost 0x1]LOG]!><time="15:30:20.084+240" date="10-30-2013" component="CcmEval" context="" type="1
<![LOG[Detecting if client is on the internet.]LOG]!><time="15:30:20.094+240" date="10-30-2013" component="CcmEval" context="" type="0" thr
<![LOG[Client is not set to use any webproxy.]LOG]!><time="15:30:20.096+240" date="10-30-2013" component="CcmEval" context="" type="0" thre
<![LOG[Client is set to use HTTPS when available. The current state is 224.]LOG]!><time="15:30:20.096+240" date="10-30-2013" component="Ccm
<![LOG[GET: Host=CLT-VSCCM-01A.NORTHAMERICA.CORP.MICROSOFT.COM, Path=/SMS_MP/.sms_aut?MPLIST, Port=80, Protocol=http, Flags=513, Options=2
<![LOG[Raising event:instance of CCM_CcmHttp_Status{    ClientID = "GUID:312D8083-89C3-48C9-A566-292C5AEB0989"; DateTime = "20131030193020.
<![LOG[Successfully submitted event to the Status Agent.]LOG]!><time="15:30:20.928+240" date="10-30-2013" component="CcmEval" context="" ty
<![LOG[Client's current MP is http://cm12cas.contoso.com and is accessible]LOG]!><time="15:30:20.928+240" date="10-30-2013" component="Ccm
<![LOG[MP check succeeded]LOG]!><time="15:30:20.928+240" date="10-30-2013" component="CcmEval" context="" type="1" thread="27008" file="eva
<![LOG[Send previous report if needed.]LOG]!><time="15:30:20.936+240" date="10-30-2013" component="CcmEval" context="" type="1" thread="270
<![LOG[Previous report was sent as state message, check whether it was really sent]LOG]!><time="15:30:20.937+240" date="10-30-2013" compone
<![LOG[Previous report was successfully sent as a state message.]LOG]!><time="15:30:21.055+240" date="10-30-2013" component="CcmEval" conte
<![LOG[Previous site code PRI, current site code PRI]LOG]!><time="15:30:21.059+240" date="10-30-2013" component="CcmEval" context="" type="
<![LOG[Client health evaluations are configured to always send data.]LOG]!><time="15:30:21.059+240" date="10-30-2013" component="CcmEval" c
<![LOG[Begin to send client health status report]LOG]!><time="15:30:22.060+240" date="10-30-2013" component="CcmEval" context="" type="1" t
<![LOG[Successfully sent client health status as a state message.]LOG]!><time="15:30:22.112+240" date="10-30-2013" component="CcmEval" cont
<![LOG[==========[ ccmeval finished normally in process 26884 ]==========]LOG]!><time="15:30:22.167+240" date="10-30-2013"
```



Real World Scenario

CCMEval–Customizable? Portable?

Contoso has around 25,000 clients who they monitor on a daily basis to ensure they are healthy. In the past, Contoso used to spend 10 hours a week troubleshooting the clients that were not reporting to the site. Now, with ConfigMgr 2012 R2 and client health, Contoso only spends about two hours reviewing the reports, alerts, and client statuses. When there is a problem, most clients automatically remediate by themselves using the `CCMEval` and `CCMrepair` task. If this doesn't fix the problem, Contoso should focus their efforts only on those clients that are failing. This is a good example of how client statuses save hours of works by implementing ConfigMgr 2012 R2.

After taking a peek at the `CCMEval.xml` and `CCMEval.log` files, a common question to ask is whether customers are able to customize or add to these checks. Unfortunately, changes to these files are not supported, so if any modifications are attempted, they are solely at the risk of the administrator and may cause problems. Remember, the content of this file impacts every Configuration Manager client in the organization.

Another question that commonly follows is whether it's possible to port the CCMEval process to work on earlier versions of Configuration Manager clients. The answer is no. CCMEval is solely for use on Configuration Manager 2012 client systems.

Client Health Evaluation: Results

Client health evaluation results are accessible in the Configuration Manager console in several areas. First, client health is reported on a device level by reviewing collection membership. Any collection in which the device is a member will provide the same health information. To view health results for a device, simply select it in the console, and the bottom of the screen will reveal five tabs: Summary, Client Check Detail, Malware Detail, Antimalware Policies, and Client Settings. All of these tabs contain useful health information, but for client health evaluation, the first three are the main ones to review.

Summary The Summary tab, shown in Figure 7.11, reports the latest client health information as Pass or Fail and also reports whether the last remediation attempt was successful.

Client Activity The Client Activity tab, shown in Figure 7.12, reports the last time the client requested policy, sent a heartbeat, reported hardware or software inventory, and sent a status message. The Days Since Last Communication field reflects how long the site has gone without hearing from the client. All of this information taken together gives a good idea about client health, but it's important to also factor in systems that may be powered off for extended periods or are offline because of network or other issues. The Management Point field documents the management point in use by the client. This information can help identify potential issues with boundaries, roaming, and the like.

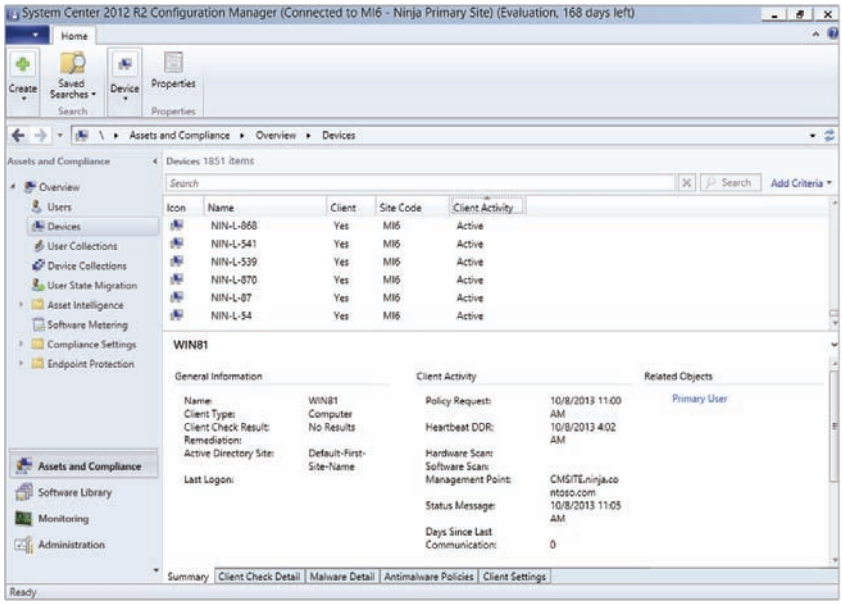


FIGURE 7.11 Summary tab for specific device

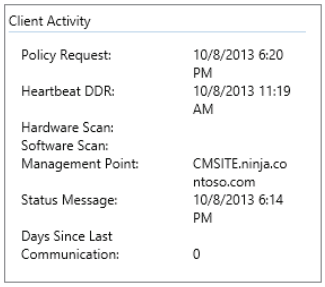


FIGURE 7.12 Client Activity Detail tab for specific device

Client Check Detail The Client Check Detail tab, shown in Figure 7.13, provides summary information about the device's last health evaluation scan. The specific evaluation rules and remediation status are reflected in the summary.

Configuring Client Health

Now that you understand the main functions of the client health mechanism and what can be remediated with CCMEval, it's time to configure client health. Before you can monitor the client status and remediate problems that are found in your hierarchy, you must configure your site to specify the parameters that are used to mark clients as inactive and configure options to alert you if client activity falls below a specified threshold. You can also disable computers from automatically remediating any problems that client status finds.

1. In the Configuration Manager console, choose Monitoring.
2. In the Monitoring workspace, select Client Status, and then right-click it and choose Client Status Settings.
3. In the Client Status Settings Properties, shown in Figure 7.14, configure the following settings:

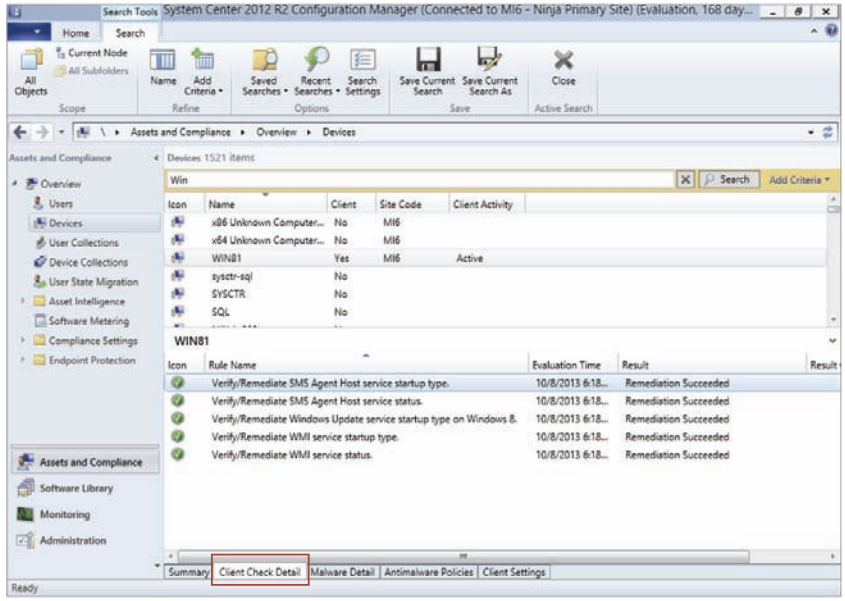


FIGURE 7.13
Client Check Detail tab for specific device

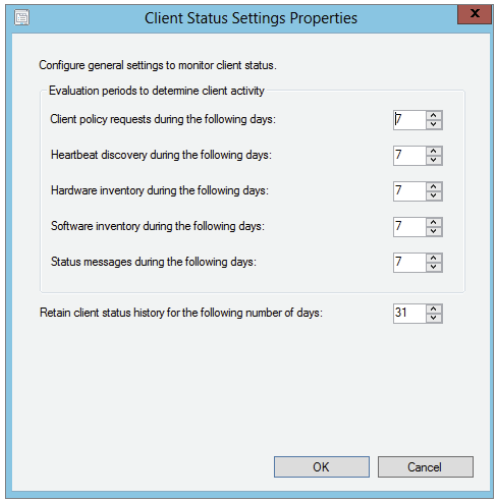


FIGURE 7.14
Client Status Settings Properties

- Client Policy Requests During The Following Days: Specify the number of days a client has requested policy. The default value is 7 days.
- Heartbeat Discovery During The Following Days: Specify the number of days the client computer has sent a heartbeat discovery record to the site database. The default value is 7 days.
- Hardware Inventory During The Following Days: Specify the number of days the client. computer has sent a hardware inventory record to the site database. The default value is 7 days.

- Software Inventory During The Following Days: Specify the number of days the client computer. has sent a software inventory record to the site database. The default value is 7 days.
- Status Messages During The Following Days: Specify the number of days the client computer has sent status messages to the site database. The default value is 7 days.
- Retain Client Status History For The Following Number Of Days: Specify how long you want the client status history to remain in the site database. The default value is 31 days.

4. Once you finish configuring each item, click OK.

Monitoring: Client Status

The Monitoring workspace of the Configuration Manager console is the place to view Client Check and Client Activity information summarized for all clients in the hierarchy. This information is located under the Client Status node.

The Client Check node shown in Figure 7.15 shows a collective view of client health in the hierarchy. The number of devices that have passed or failed or are in an unknown status for health evaluation are reflected in a pie chart, and the accompanying legend details issues that have been found for those systems failing health evaluation. There is also a line graph showing trending information for client health. For more detail simply click the section of interest from the pie chart, the pie chart legend, or the line graph, which will open a view of all devices in the selected category.

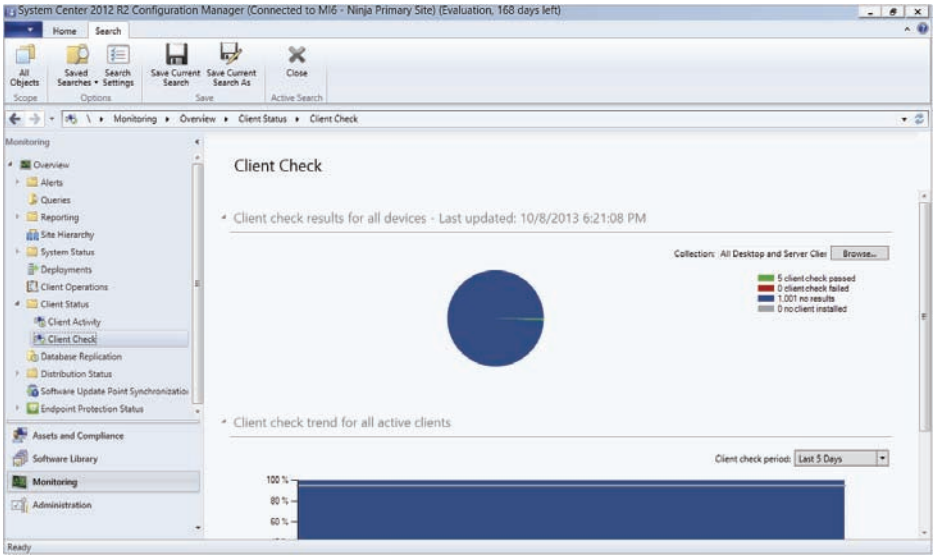


FIGURE 7.15 Client Check node in the Monitoring workspace of the Configuration Manager console

Monitoring: Client Activity The Client Activity node shown in Figure 7.16 shows a collective view of client activity in the hierarchy. Devices are represented in a pie chart as either active or inactive. In the example, all clients are active. Having 100 percent active clients would be a *great* result in a production environment but likely will not often be achieved because of environmental issues, systems being powered off for extended periods, network issues, and the like. This view also provides a line graph for trend analysis. To view specific systems that are in an active or inactive state, simply click the area of the pie chart or pie chart legend of interest to drill down for additional detail.

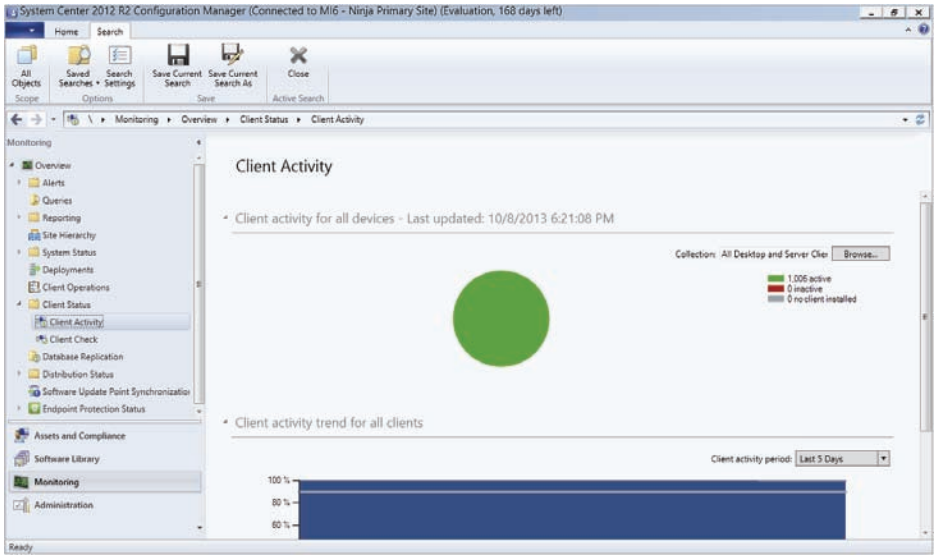


FIGURE 7.16 Client Activity node in the Monitoring workspace of the Configuration Manager console

Reporting: Client Status Configuration Manager 2012 provides a wealth of information through the reports available in the console. Reports are grouped by category and, as shown in Figure 7.17, there are seven reports specifically geared to client status information. Combining the reports with the ability to create report subscriptions, as detailed in Chapter 13, "Reporting," gives administrators significant flexibility to pick reports that best serve their needs and render or deliver automatically.

Alert: Client Health

Part of being a ConfigMgr administrator is that you don't have enough time to perform all of your daily task, weekly, and monthly tasks. The monitoring aspects of client health are a very good method of keeping you informed about what is going on with your clients. With

ConfigMgr 2012 R2 you have the ability to configure alerts for each collection. If you use this method to find out what is going on with your clients, then you can focus on those critical systems. To configure the alerts that will be displayed on the Monitoring workspace, perform the following steps on those critical collections:

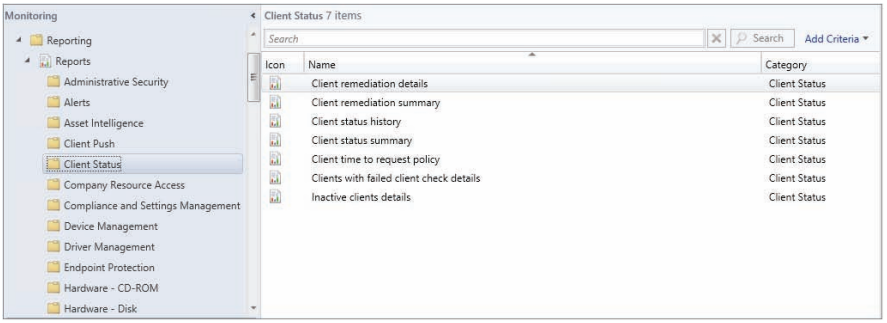
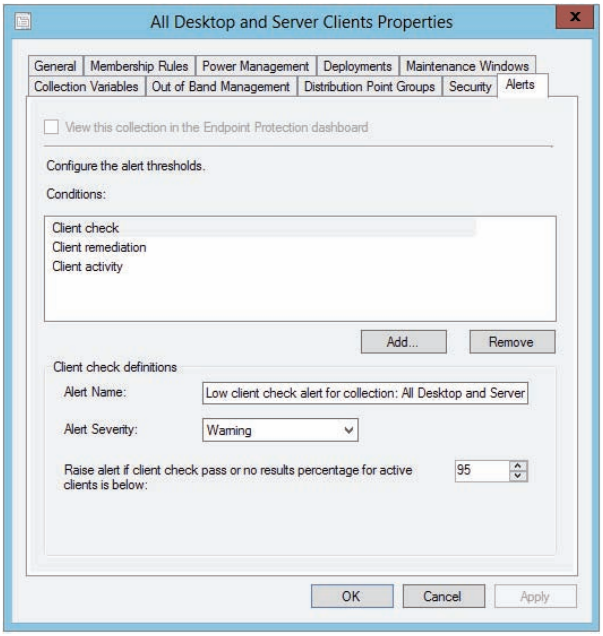


FIGURE 7.17
Client Status reports

1. In the ConfigMgr console, select Assets And Compliance.
2. In the Assets And Compliance workspace, choose Device Collections.
3. In the Device Collections node, select the collection for those critical systems and right-click Properties.
4. In the Properties dialog box, click the Alerts tab, as shown in Figure 7.18, and then click Add.
5. In the Add New Collection Alerts dialog box, choose the alerts that you want generated when the client status thresholds fall below a specific value. Then click OK.
6. In the Conditions list, select each client status alert and then specify the following information:
   - Alert Name: Accept the default name or enter a new name for the alert.
   - Alert Severity: From the drop-down list, choose the alert level that will be displayed in the Configuration Manager console.
   - Raise Alert If Client Check Pass Or No Results Percentage For Active Clients Is Below: Specify the threshold percentage for the alert.
7. Click OK.

Figure 7.18
Client health collection alerts



The Bottom Line

Detail client health evaluations in Configuration Manager 2012 R2. Health evaluations and remediations take place daily on every Configuration Manager 2012 client in the hierarchy. This information is updated at the site and is available for review on every client and also summarized for every client across the hierarchy.

Master It List the health evaluations and remediations that take place on Configuration Manager clients.

Review client health results in the Configuration Manager console. Client health data is available in several locations of the console to allow access to health for individual devices and summarized data for all clients in the hierarchy.

Master It List the locations in the console where individual client health and summarized client health data are accessible.



Chapter 8

Application Deployment

The ability to deploy applications has long been a primary function of Configuration Manager. The Application Deployment feature of Configuration Manager 2012 is the new approach for software deployment and allows administrators to deploy almost any kind of content to Configuration Manager clients, affecting potentially thousands of systems or users.

The list of content deployable through Application Deployment includes virtually anything—from full applications (i.e., Office) to scripts and batch files. Beyond simply specifying *what* to deploy is also the ability to detail *how* to deploy, including whether an application should be delivered to systems versus users or whether the application should be a full installation on the target system versus a virtualized version using App-V.

With so much flexibility and power comes a great amount of responsibility. Configuration Manager provides robust ability to define and control Application Deployment to systems and users. When properly used, the experience with Application Deployment will be very positive, but it is also possible to make mistakes with this feature and deliver the mistakes to potentially thousands of systems or users. This underscores the need to completely understand the feature and its various options and also the need for proper testing before introducing a change to such a potentially large number of systems or users. This need for proper understanding and testing is not unique to Configuration Manager but applies to any product of enterprise scale.

This chapter will detail the various options and features of Application Deployment in Configuration Manager 2012.

In this chapter, you will learn to

- Explain the options available for Application Deployment
- Detail the various components required for Application Deployment
- Understand the role of and manage distribution points

What's New in Application Deployment?

The label *Application Deployment* describes the new approach being taken in Configuration Manager 2012 for deploying content. Software Distribution, as it has been historically known, has not been removed from the product; it is still present in the console and represented by the Packages node of Application Management. Also note the Applications node, which is where configurations using the new approach are centered. This is shown in Figure 8.1.

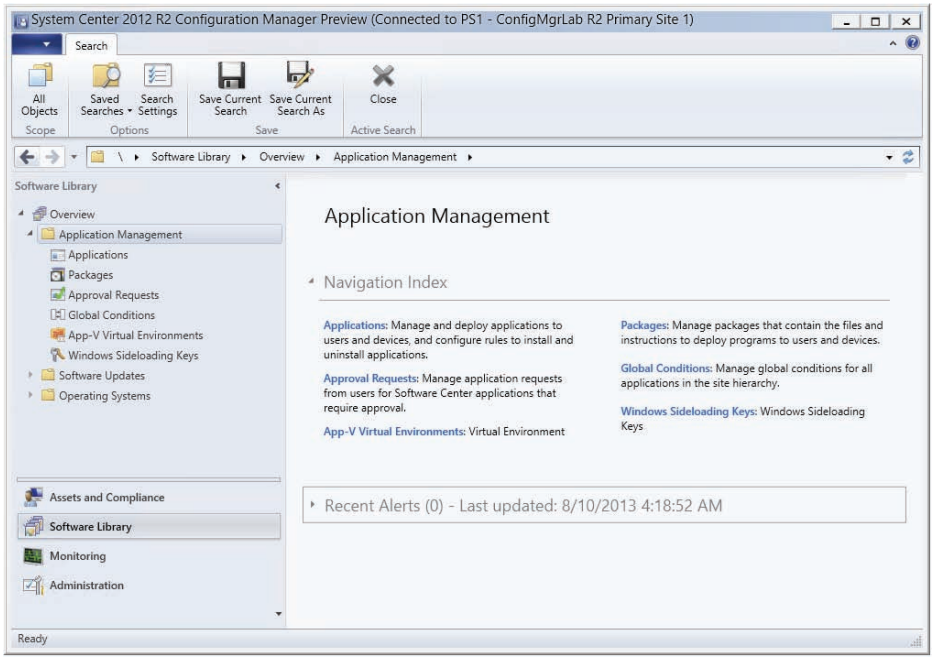


FIGURE 8.1 Applications and Packages nodes

Classic Software Distribution works very much the same way as it did in Configuration Manager 2007. Classic Software Distribution might be seen as available only to facilitate migration and to allow administrators the ability to deploy content the old way while learning the new approach in Configuration Manager 2012. Classic Software Distribution actually remains very useful in certain scenarios. Remember that the new Application Deployment approach is designed to deploy applications, and it offers very rich configurations. The Application Deployment model, however, may not be a good option for every potential deployment. Consider a scenario where an administrator simply needs to deploy a command line to systems. The Application Deployment model isn't well suited for such a task, and instead administrators should use either classic Software Distribution or a task sequence. Classic software packages can be migrated to the new application model with the Package Conversion Manager discussed in Chapter 3, "Migrating to Configuration Manager 2012."

With proper deference given to classic Software Distribution, it is much the same as it was in Configuration Manager 2007, so the discussion in this chapter will be solely focused on the new Application Deployment features.

If you need a full review of the classic Software Distribution model, an excellent discussion is available in the book *Mastering Microsoft System Center Configuration Manager 2007 R2* (Sybex, 2009).

Note the difference in terminology, as shown in Table 8.1.

Table 8.1: Terminology differences

Application Deployment	Classic Software Distribution
Application	Package
Deployment type	Program
Deployment	Advertisement

Because Application Deployment is such a paradigm shift from classic Software Distribution, a bit of discussion about what exactly has changed is warranted.

Distribution Point Changes

Distribution points are key components for any kind of content delivery in Configuration Manager. Understanding the changes to and optimizations of this role will directly relate to the efficiency of your design and satisfaction with the product.

Workstations as Distribution Points Branch distribution points were first introduced in Configuration Manager 2007, and as of Configuration Manager 2012 they are gone! Don't worry though; they have been replaced with the ability to directly configure any Windows 7 workstation as a distribution point. This may seem like simply a cosmetic difference—and in some ways that is true, but not totally—there are some significant differences.

The ability to specify a workstation as a distribution point directly means that instead of having a client component to fill the distribution point role, as was the case with Configuration Manager 2007 branch distribution points, now the client doesn't even have to be present!

One limitation of distribution points located on workstation systems is the limit of 20 simultaneous connections. This is a workstation operating system limitation rather than a limit imposed by Configuration Manager.

Single Instance Storage The traditional distribution point structure and function are still available for very specific classic Software Distribution scenarios, namely, if a legacy package is configured to run from a distribution point. For every other kind of content deployment, whether classic Software Distribution or the new Application Deployment model, the distribution point engine is completely new. The change also brings some changes in administration, but they are well worth it!

Content storage on traditional distribution points often requires substantial hard drive space. The new distribution point model takes advantage of single-instance storage, which will result in less hard drive space required for content. There are a couple of things to note as a result of this change:

- Administrators or users are no longer able to connect to a known distribution point and execute an install remotely.
- The Run From Distribution Point option is not available for Application Deployment (but is still available with classic Software Deployment).
- The single-instance storage change increases security by obscuring the content and making it difficult for the content to be downloaded and used other than for the intended purpose.

Distribution Point Content Validation Many Configuration Manager administrators have faced the problem where content initially deploys to distribution points but later becomes corrupt, preventing further deployment until the corruption is resolved. Often the only way administrators have known about the corruption is through failed deployments. Configuration Manager 2012 offers the ability to proactively check content for corruption on both classic and new distribution points and, when found, notify the administrator so proactive corrective action may be taken.

Remote Distribution Point Throttling A common reason for maintaining secondary sites in a Configuration Manager hierarchy is to support locations where it is important to ensure that network bandwidth usage is tightly controlled when sending content to locations with slow, overloaded, or unreliable WAN connections.

Configuration Manager 2012 allows throttling of bandwidth directly between a site and its remote distribution points, helping eliminate the need for secondary sites to achieve this goal.

Hierarchy simplification was a design goal for Configuration Manager 2012. This one added feature helps achieve the simplification goal by drastically reducing the need for secondary sites in most Configuration Manager 2012 hierarchies.

Distribution Point Selection The ability to specify which distribution points are available to clients, an option known as *protected distribution points,* has been available in previous versions of Configuration Manager.

In Configuration Manager 2012, all distribution points are protected by default. The only way clients are able to access a distribution point is if the distribution point is part of a boundary group that matches the client's current boundary. There is a fallback mechanism to allow clients to access distribution points when the client is in an unknown boundary. Allowing fallback is configured per distribution point and per deployment.

Prestaged Content Managing content in bulk on distribution points has historically been challenging for Configuration Manager administrators. When replacing a distribution point server or even simply renaming, replacing, or modifying hard disks, administrators were faced with the need to redistribute all content to the new server. If connectivity to the server in question was either unreliable or slow, the challenge was even more pronounced.

An initial thought to solve the problem might be to simply copy content from the current to the replacement server. A quick evaluation of this option reveals that it is not a workable choice because a simple file copy does not result in the needed database and other adjustments to reflect the new location of the content. Because of this, administrators either had to use external tools, such as `preloadpkgonsite.exe`, or suffer through overloading the network while copying potentially gigabytes of content.

Configuration Manager 2012 introduces an option allowing content to be prestaged on distribution points. There is a specific wizard used to accomplish this—as will be seen later in the chapter—but the net effect is that in situations where bandwidth is challenging, content can now be natively staged locally on systems without such strain on network links.

Distribution Point Groups The process of either adding or replacing a distribution point in Configuration Manager is fairly straightforward, but what about the content? If the distribution point being replaced is the storage point for many applications, administrators historically

have been faced with either constructing a script to parse through applications and adding them to the new distribution point in bulk or working through applications one by one and enabling the new distribution point. Either task is time consuming!

The use of distribution point groups was possible in Configuration Manager 2007 but was not often used by administrators. Configuration Manager 2012 revamps the use of distribution point groups, and they now take center stage and offer very easy management of distribution points by allowing distribution points that should store similar content to be treated collectively. Simply choose a distribution point group when deploying or removing content, and all distribution points within that group will receive or remove the content. Better still, when a new distribution point is added to the group or removed, then all applicable content targeted to the group will also be added or removed.

User-Centric Focus In previous versions of Configuration Manager it was possible to target a deployment to users, but this ability was not robust and seemed like an afterthought. In Configuration Manager 2012, the user is the focus—or at least can be.

Yes, it is still possible to target deployments to systems, and many administrators will continue to do this because, in many cases such as server management, that is the best approach. Plus, the ability to target users for deployments and to do so with great specificity is a paradigm shift for Configuration Manager. Don't overlook this feature though, because it offers the ability to significantly enhance a user's experience with and impression of Configuration Manager.

User-centric focus allows administrators to define deployments that function differently based on the location of the user. Consider, for example, a user who is logged onto and using their main computer (known as a primary device in Configuration Manager terminology). Deployments can be configured to recognize this and, in such cases, install software directly onto the user's device, including mobile devices managed directly or via Windows Intune—more on that in Chapter 16, "Mobile Device Management." Conversely, if the user happens to be logged onto a device in another location, such as in a remote office, this can be recognized and the deployment can be delivered automatically as a virtualized application instead, allowing the deployment to be made available quickly and without persisting the installation. This allows the user the same experience regardless of which system they are actually logged onto and using, and it's all seamless.

Software Center The Configuration Manager Software Center is an updated replacement to the Run Advertised Program option available in previous versions of Configuration Manager. The Software Center is the central location where users are able to view available or required deployments targeted for their system and to also make their own custom changes such as to specify working hours or whether Configuration Manager operations should be suppressed while presentations are taking place, or even whether their computer should honor assigned power-management settings.

The only required deployments visible in Software Center will be those that are configured with the ability for users to interact.

Application Catalog This often-requested and long-awaited feature is finally here! Configuration Manager 2012 allows administrators an option to publish deployments into a web-based Application Catalog. The Application Catalog web page is accessible to any user and is filtered to list only deployments specifically targeted to the given users. Through the catalog, users

are able to request available software that is of interest. Entries in the Application Catalog can be configured as freely available or as requiring approval. Note the Approval Requests node under Application Management in Figure 8.1. When software is configured to require approval, the user is able to request the software, but an administrator will need to manually approve the request before deployment will continue. Administrators approve pending requests in the Approval Requests node.

Applications: Application References

The Application References mechanism allows administrators to view what dependency and supersedence relationships are associated with a given application. The best way to describe this is by example.

Dependency Assume two applications, Foxit Reader and .NET Framework 2.0. It is possible to specify a dependency so that Foxit Reader requires that .NET Framework 2.0 be present on a target device. If .NET Framework 2.0 isn't present on the device when you attempt to deploy Foxit Reader, you can configure it to automatically deploy as part of the Foxit Reader deployment. If not, Foxit Reader will fail to install until .NET Framework 2.0 is present.

The dependencies themselves are configured on the Dependencies tab of the properties for the application deployment type. The References tab on the application properties dialog box simply displays the information for the application as a whole.

Supersedence Assume two applications, Foxit Reader and Adobe Acrobat 9 Pro. It is possible to specify a supersedence relationship to define that Foxit Reader supersedes Adobe Acrobat 9 Pro. Doing so effectively links the two applications and establishes a path for replacing one application with another, either by upgrade or by uninstalling the superseded application and replacing it with the current application.

Be careful when building relationships between applications. Relationships will prevent an application from being deleted, and excessive numbers of relationships will increase complexity and potential confusion.

Deployments

Deployments in Configuration Manager 2012 directly influence the flow of application deployment. There are a number of new options available to help control this flow, as described here:

Deployment Types Deployment types specify how a particular application should be deployed. As shown in Table 8.1 previously, think of deployment types as similar to programs in classic Software Distribution but with much greater flexibility and specificity. There are multiple deployment types available.

- Windows Installer (`.msi` file)
- Windows app package (Windows 8.*)
- Windows app package in the Windows Store

- Script Installer
- Microsoft Application Virtualization version 4
- Microsoft Application Virtualization version 5
- Windows Phone app package (`.xap` file)
- Windows Phone app package in the Windows Phone Store
- Windows Mobile Cabinet (`.cab` file)
- App Package for iOS (`.ipa` file)
- App Package for iOS from the Apple App Store
- App Package for Android (`.apk` file)
- App Package for Android on Google Play
- Nokia SIS file
- Mac OS X (`.cmmac` file)
- Web Application (URL)

Beyond these predefined types it is possible to manually define whatever other type of deployment may be needed.

Native Uninstall Support Previous versions of Configuration Manager allowed for software deployment but no native support for software uninstall. Uninstall was possible but required a separate program definition. Configuration Manager 2012 allows specifying options for both install and uninstall within a single deployment type. There is no requirement to use both, but they are available. When you create an application using the wizard, some deployment types—such as MSI-based deployments—will automatically create the uninstall option.

Detection Method Previous versions of Configuration Manager allowed administrators to define a deployment but no mechanism to determine if that deployment had already taken place by another mechanism. The result was that software could get reinstalled even if it was already present. Configuration Manager 2012 allows administrators the ability to define rules to determine if the deployment is already in place on a system and, if so, to simply exit without triggering a reinstall. This mechanism may seem similar to what historically has been seen with software patching. The two mechanisms are very similar.

Requirements In previous versions of Configuration Manager it was common practice to build collections of systems matching specific criteria or filters and then to target advertisement(s) to those collections. In Configuration Manager 2012, collections remain a requirement for deployment targeting, but the need to build a new collection or multiple new collections to provide filtering for a single deployment should be reduced. Administrators now have the ability to specify deployment requirements per deployment type. These require-

ments ensure a specific deployment type is not executed unless specific criteria are met. Once defined, requirement rules are reusable.

Targeting

Historically it has been recommended to avoid targeting the All Systems collection when deploying software. Doing so meant that the software would be received and executed by every device that is part of the All Systems collection, which is every device at a site and potentially every device in the hierarchy. It is still a good idea to avoid targeting the All Systems collection, but with deployment type requirements properly configured, it would be possible to safely do so if needed.

Dependencies The ability to specify dependencies between different deployments has been available since the release of SMS 2.0. Until Configuration Manager 2012, however, these dependencies were not so straightforward and creating multiple dependencies often resulted in confusion.

Dependencies in Configuration Manager 2012 are a much more elegant solution and allow administrators to configure other applications on which the one being configured depends. Single dependencies may be specified or multiple. When adding dependencies it is possible also to select whether a given dependency will be automatically installed in the event it is absent. Setting Auto Install for a dependency is not a requirement but can help ensure deployments execute error free.

Adding dependencies essentially joins the current application with whatever dependency is being specified, so later, if a dependent application is removed, a warning will be displayed about potentially breaking a dependency relationship.

While dependencies are a big step forward for controlling and predicting application deployment results, there is still no way to define order of installation for dependencies. Typically this fact isn't a big deal, but if multiple dependencies are configured for an application, it could be a concern. If it is required to know the exact order of execution for a deployment and its related dependencies, consider using a task sequence instead.

Return Codes A successful install of most applications will result in a return code of either 0 or 3010 being generated. These return codes mean success or success pending reboot, respectively. In previous versions of Configuration Manager, if a return code other than these two is returned, then the application deployment is considered to have failed. Depending on the software manufacturer, a return code other than 0 or 3010 may actually be informative about the state of a deployment other than simply indicating success or failure. The number of such applications is relatively small, but when encountered they can be frustrating because a successful install will appear to have failed. The task sequence engine in Configuration Manager 2007 was the first place where administrators were able to account for exit code variations. In Configuration Manager 2012 this ability has been brought forward to Application Deployment as well, fully allowing administrators to define what specific exit codes from an application actually mean and responding accordingly when reporting status.

Deployment Settings Action Previous versions of Configuration Manager allowed deployments to be built that would be installed on clients. Configuration Manager 2012 also allows for that but introduces the ability to force an application uninstall on clients. This action will cause the uninstall command line configured on the deployment type to be executed.

Deployment Settings Purpose The deployment purpose can be configured as either available or required. These options are similar to specifying a deployment as optional or mandatory in previous versions of Configuration Manager, but with a twist. When a deployment is configured as required, the application will be forced onto the client. This is the same behavior as previous versions when selecting a mandatory deployment. The twist is that on a schedule, the deployment is reevaluated, and if the application is found to be missing, it is forced back onto the client system.

Alerts New to Configuration Manager 2012 is the ability to specify alerts when deployments fail to reach a certain threshold of success, specified as a percentage. The next question that often is asked when discussing this new alerting functionality is whether this ability is intended to replace monitoring by the System Center Operations Manager Configuration Manager 2012 management pack. The answer is a resounding no. The scope of the Configuration Manager 2012 management pack is more encompassing than what can be achieved by native Configuration Manager 2012 alerting. The alerting feature in Configuration Manager 2012 is introduced to allow administrators some ability to raise awareness of issues independently without System Center Operations Manager. In environments with System Center Operations Manager, the Configuration Manager 2012 management pack should be the primary monitoring resource, with the internal Configuration Manager alerting engine acting as a supplement.

Dependencies for Application Deployment

The Application Deployment feature makes use of several different dependencies. These dependencies must all be configured correctly for application deployment to be successful.

Management Point

The management point is the key interface between clients and their assigned site. Through management point policy updates, clients learn about assigned settings and activity requested by the site and also return data to the site, such as inventory or discovery data. It is through management point policies that clients are made aware of pending application deployments and associated settings, and it is through the management point that clients return status after attempting to run an application deployment. It is also through the management point that clients look up which distribution points are available when it comes time to execute an application deployment.

Thus, having a functioning management point is crucial not only for proper client operation but also for proper application deployment. Chapter 4, "Installation and Site Role Configuration," includes full discussion of management point setup and configuration.

Distribution Point

The distribution point role is crucial for application deployment in that it is the location where all remote content that should be accessed and used during application deployment is stored. If a distribution point is not available to clients when you attempt to initiate an application

deployment, the deployment will fail. Multiple distribution points may be present per primary site, including workstation-class machines running Windows 7 or greater. Distribution points installed for a site but on servers other than the site server, also known as remote distribution points, may be configured for content throttling in the distribution point's properties. Chapter 4 includes full discussion of distribution point setup and configuration.

Application Deployment Failure

It is possible that an application deployment may fail even if content is available on some or all of the distribution points. In such cases verify that at least one distribution point within the client's boundary is configured with content and, if the distribution point is running on a workstation system, ensure that it is not exceeding its connection limit. In addition, check whether the errors have been encountered when staging content to distribution points.

BITS-Enabled IIS

In previous releases of Configuration Manager it was optional to enable Background Intelligent Transfer Service (BITS) for a distribution point. In Configuration Manager 2012 BITS is required.

Default Client Settings

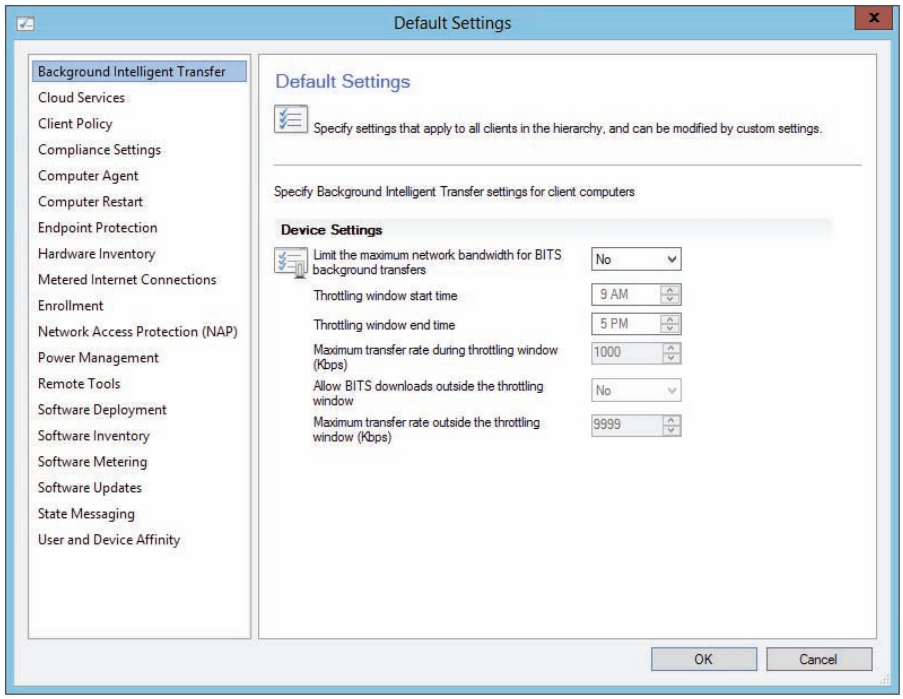
A word about client settings: The default list of client settings applies to all clients in the Configuration Manager 2012 hierarchy. It is possible to override the default settings and specify different values for specific sites or specific systems via collection targeting.

This flexibility allows administrators complete control of which settings apply to devices and removes the technical limitation that often resulted in multiple sites or hierarchies, such as scenarios where servers and workstations needed separate management settings. The flexibility offered with client settings applies generically throughout Configuration Manager, but several settings that are available have specific impact with Application Deployment, as discussed in the following sections.

Background Intelligent Transfer

BITS settings are part of the default client settings and are shown in Figure 8.2. In some environments clients are installed and managed across slow or heavily utilized WAN links. In such cases it may be important to ensure clients are able to sense a heavy load on the network and, during critical times, respond by reducing the amount of data that is being transferred, a process also known as throttling. Throttling controls are found throughout Configuration Manager 2012 to help reduce WAN impact. The BITS client settings specifically allow administrators to configure clients to limit the amount of network bandwidth they utilize when transferring content. This content includes application deployment data, along with several other types of information.

Figure 8.2
BITS settings



Real World Scenario

Configuring BITS Will Give You Good Options for Bandwidth Control

Configuring BITS settings through the client settings mechanism is very flexible and gives administrators good options for bandwidth control. These settings alone will work to achieve the desired result in most environments. Where these settings by themselves are not sufficient, it is also possible to introduce throttling directly through controls in Internet Information Server. While throttling through IIS is useful and easy to configure, it universally impacts traffic to and from IIS and should be considered only after other options have been exhausted.

Computer Agent

Computer Agent settings are part of the default client settings and are shown in Figure 8.3. These settings apply to all deployments, including software updates and operating system deployments, and allow the administrator control over the user experience while deploying content.

The Computer Agent settings can be set up in different ways, depending on the types of clients in your environment. Types of clients can be laptops, desktops, kiosks, RDP clients, or

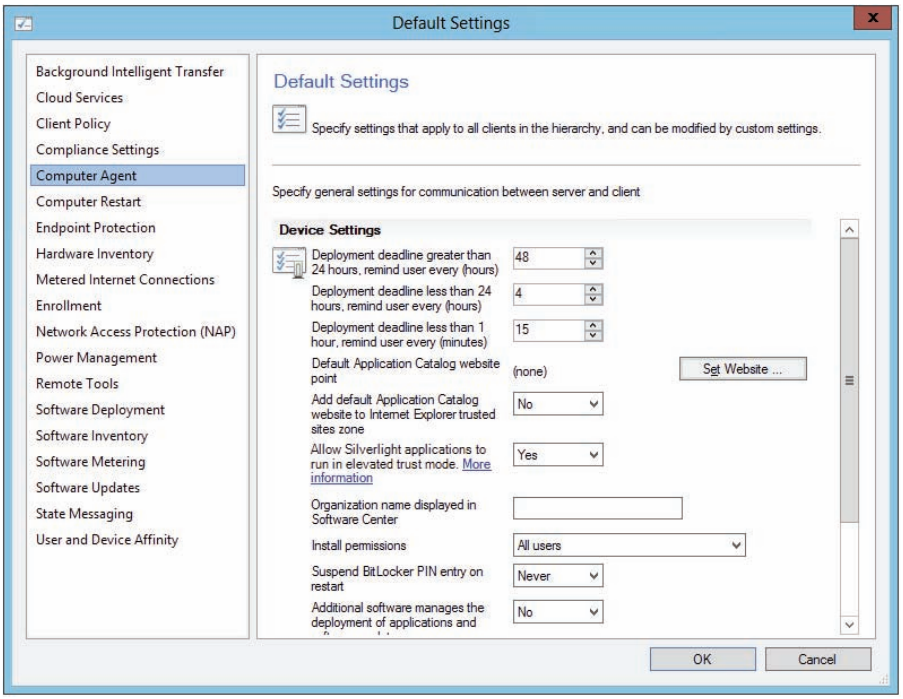


Figure 8.3
Computer Agent settings

VDI clients. In Table 8.2 you will find the options that can be configured with the Computer Agent settings.

Table 8.2: Computer Agent settings

Option	Description
Deployment Deadline Greater Than 24 Hours, Remind User Every (Hours)	Every required deployment has a deadline; when this deployment has been received by the client, you can configure how often the user must be notified when the deadline is farther away than 24 hours. This reminder will help the user to run the deployment at the time it is most suitable for them.
Deployment Deadline Less Than 24 Hours, Remind User Every (Hours)	When a deployment comes within the period of 24 hours before the deadline, you can remind the user more often, every x hours.
Deployment Deadline Less Than 1 Hour, Remind User Every (Minutes)	If the user hasn't run the deployment within one hour before the deadline, you can remind the user every x minutes. If the deadline is reached, the installation will start.

Option	Description
Default Application Catalog Website Point	When using the Application Catalog to allow users to select and install the applications they need, you are able to configure one of the available Application Catalog website points or a URL that can, for instance, be available through a network load balancer.
Add Default Application Catalog Website To Internet Explorer Trusted Sites Zone	To be able to install applications via the Application Catalog website, your Internet browser needs to trust the website. With this setting you can automatically configure the Application Catalog website to be recognized by the trusted sites zone within Internet Explorer. Adding the website to this zone will also take care of pass-through authentication to the website.
Allow Silverlight Applications To Run In Elevated Trust Mode	This setting is new for SP1 and R2 and must be enabled when using those versions. The Application Catalog website is a Silverlight application that needs to run in elevated trust mode.
Organization Name Displayed In Software Center	You can customize the Software Center by adding the company name.
Install Permissions	The Install Permissions option allows you to configure how users can initiate the installation of software, software updates, and task sequences. This option comes with four levels: ◆ **All Users** When this option is selected, all users who are logged on to the client can initiate an installation of software, software updates, and task sequences via the Software Center. ◆ **Only Administrators** When this option is selected, only users who are local administrators and who are logged on to the client are able to initiate an installation of software, software updates, and task sequences via the Software Center. ◆ **Only Administrators And Primary Users** When this option is selected, only users who are local administrators or are the primary user of the client that they are logged on to are able to initiate an installation of software, software updates, and task sequences via the Software Center. ◆ **No Users** When this option is selected, no users are able to initiate the installation of software, software updates, and task sequences via the Software Center. This option is often used when a user logs on to a Remote Desktop Services server that is shared with other users.

TABLE 8.2: Computer Agent settings *(CONTINUED)*

OPTION	DESCRIPTION
Suspend BitLocker PIN Entry On Restart	If you need to enter a BitLocker PIN when logging on to your clients, this option can bypass this requirement when the client needs to restart after a software installation.
Additional Software Manages The Deployment Of Applications And Software Updates	This option allows you to disable the deployment of applications and software updates on servers that are, for instance, used for Citrix XenApp, XenDesktop, or another shared VDI desktop solution that is using a shared image without disabling the Configuration Manager 2012 client. Tooling of the vendor will control the installation of the available deployments.
PowerShell Execution Policy	PowerShell scripts can be used to deploy software but also to check for the existence of software or to detect configuration items and check them for compliance. With this setting you can configure the execution policy for PowerShell scripts that run via the Configuration Manager client.
Show Notifications For New Deployments	You can enable or disable notification for new deployments that become available when a user is logged on to a client.
Disable Deadline Randomization	This option checks whether the client uses an activation delay of up to two hours to install required software updates and applications when the deadline is reached. By default the activation delay is disabled. For VDI environments it can help to not have to install an update on all VDI desktops at the same time. Disabling deadline randomization in big environments can negatively impact the performance of the VDI environment as well as the network, distribution points, and site servers.

Computer Restart

Computer Restart settings are part of the default client settings and are shown in Figure 8.4. These settings apply to all deployments, including software updates and operating system deployments, and allow administrators to define countdown settings to be used in the event a computer must be restarted as a result of application deployment.

Software Deployment

The Software Deployment settings are also part of the default client settings and are shown in Figure 8.5. The only option here allows administrators to determine what schedule should be used for reevaluating deployments.

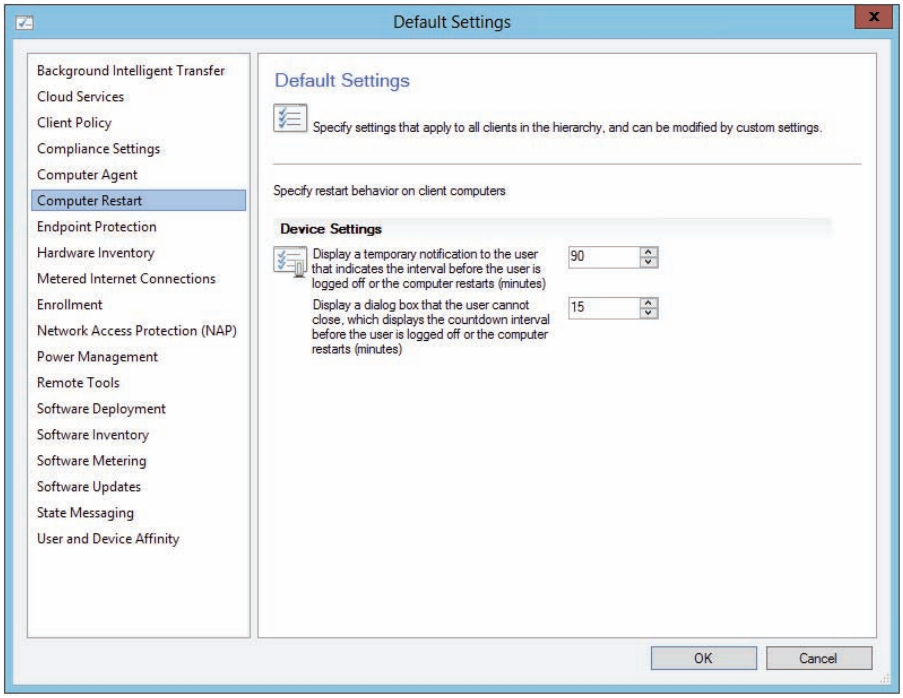


Figure 8.4
Computer Restart settings

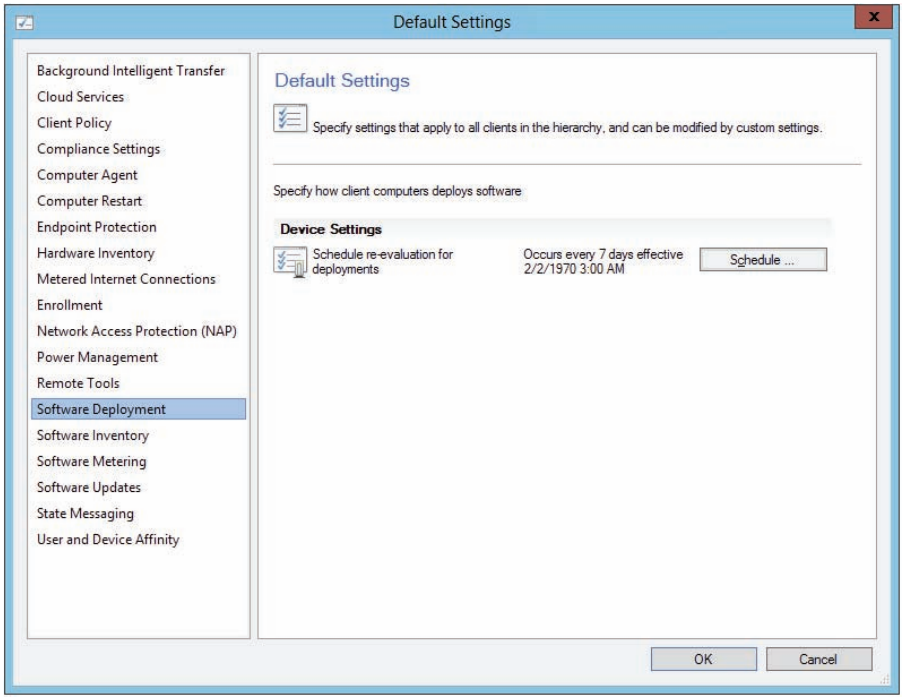


Figure 8.5
Software Deployment settings

When you, as a Configuration Manager administrator, decide to uninstall, for instance, an expensive version of Autodesk AutoCAD from your clients and a user then decides to reinstall the same version, they may make it so you are no longer compliant with your licenses.

When reevaluating the client, Configuration Manager will see that AutoCAD is installed on the client and will automatically uninstall it again.

User and Device Affinity

The User and Device Affinity settings are also part of the default client settings and are shown in Figure 8.6. These settings specify options that Configuration Manager 2012 will use when attempting to determine whether a user is logged onto a primary device or logged on elsewhere.

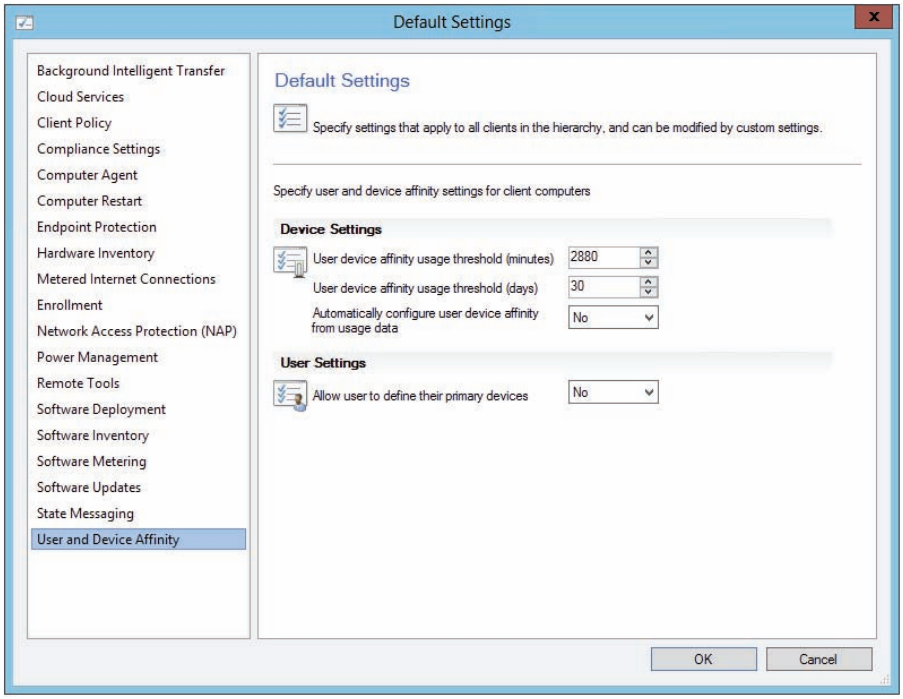


Figure 8.6
User and Device Affinity settings

Software Distribution Properties

Software Distribution properties are accessible from the Administrative node by selecting Administration ➢ Overview ➢ Site Configuration ➢ Sites and then selecting a site server hosting distribution points. From the ribbon select Configure Site Components and then Software Distribution. This option allows administrators to configure concurrent package distribution settings and also retry settings if a failure is encountered. These settings are the same as what were available in previous versions of Configuration Manager.

The Network Access Account, shown in Figure 8.7, is used to define an account that can be used for network access when content is needed during deployment from a network location other than the Configuration Manager distribution point. The Network Access Account also is used in scenarios where clients are installed in an untrusted scenario, such as workgroup systems or machines in an untrusted forest. This account is also key for use in operating system deployment. With Configuration Manager 2012 R2 you can create more than one Network Access Account per site. When a client tries to access content and cannot use its local computer account, it will first use the last Network Access Account that was able to successfully connect to the distribution point. Configuration Manager supports adding up to 10 Network Access Accounts. The ability to add more than one Network Access Account to one site offers an option to simplify the Configuration Manager 2012 hierarchy, since the Network Access Account could be one of the reasons for installing more than one primary site.

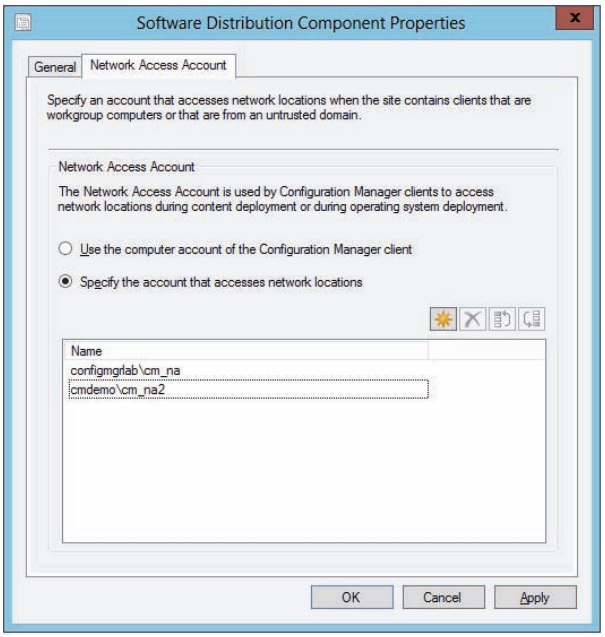


Figure 8.7
Software Distribution Component Properties

SQL Data Replication

Previous versions of Configuration Manager made use of standard site-to-site communications for sending all data between sites. Configuration Manager 2012 still uses site-to-site communications for some data, but for configuration data, such as application deployment configurations, that data is replicated between sites using SQL Server features. Thus, ensuring that the SQL data replication structure for Configuration Manager 2012 is healthy is key to guaranteeing consistent data throughout the hierarchy.

Site-to-Site Communications

The mechanism for site-to-site communications has been part of Configuration Manager for many versions. This mechanism is much the same in Configuration Manager 2012, but its scope is limited to sending data such as application deployment content. SQL data replication is used for transferring site settings information.

Collections

Collections remain integral to application deployment. Collections are the ultimate target for all deployments, and so the proper use of collections, including dynamic versus static collections, and the proper replication of collection data between sites via SQL data replication are key to successful application deployment.

Proper use of collections is crucial for successful application deployment, but collections are necessary to many functions in Configuration Manager 2012 beyond just application deployment. For that reason, collection management and strategy are not discussed in this chapter but are discussed in more detail in Chapter 17, "Role-Based Administration."

Boundaries/Boundary Groups

Boundaries and boundary groups are the mechanisms Configuration Manager 2012 clients use to locate available distribution points for content access. Configuring these settings correctly will allow for efficient application deployment. Boundaries and boundary groups are detailed in Chapter 2, "Planning a Configuration Manager Infrastructure."

Elements of Application Deployment

Several components are integral to successful configuration of Application Deployment in Configuration Manager 2012. Some of these components are specific to Application Deployment and others apply more generally. In either case, a proper understanding and configuration of these components are important.

Applications

Administrators build applications in Configuration Manager 2012 to describe software that is to be deployed. Administrators create an application to specify details regarding the application, such as the manufacturer, an internal contact for support, information that should appear in the Application Catalog, details regarding the action an application will take, or whether the application being built supersedes a previous version.

A sample application is shown in Figure 8.8. The process of building an application will be detailed shortly.

Deployment Types

The act of creating an application by itself does not specify sufficient instruction for carrying out deployment of the application. Deployment types provide additional detail for how a given application should be handled in various situations, such as what type of action to take when the application is being deployed to various types of devices or users. In addition, a deployment type also describes mechanisms to detect whether an application is already installed or command lines needed to remove an application. The deployment type is created

when building an application through the Create Application Wizard, so the difference between the application itself and the deployment type may not be clear. Figure 8.8 shows the General Information tab for the application definition. The Deployment Types tab, which will list all configured deployment types for the application, is also visible in Figure 8.8. Figure 8.9 shows the properties of a sample deployment type. The process of building deployment types will be detailed shortly.

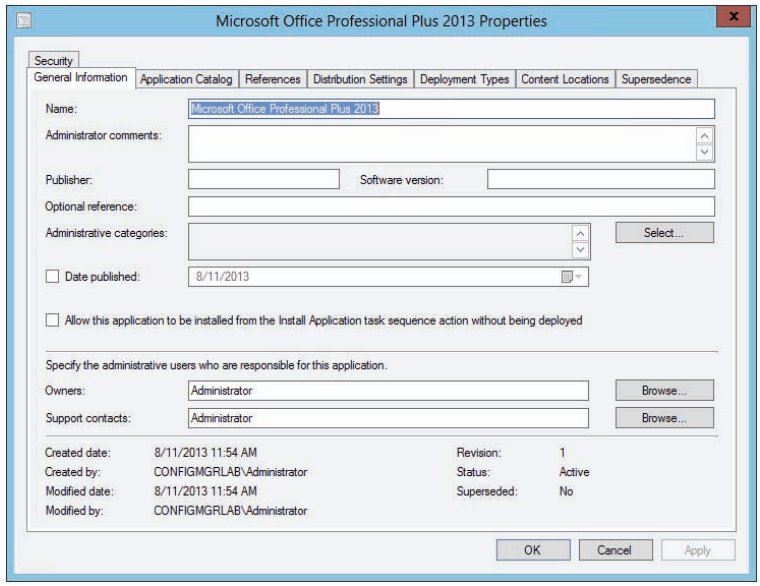


Figure 8.8
Sample application properties

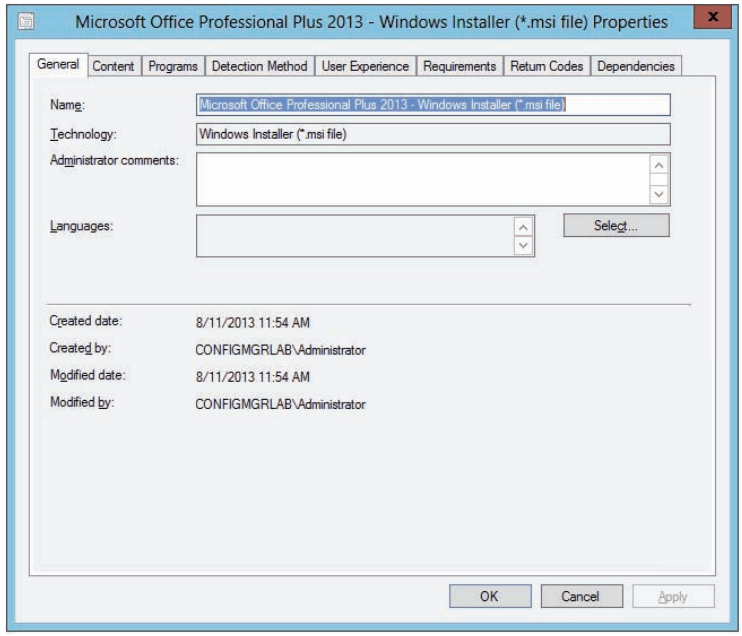


Figure 8.9
Sample deployment type properties

Deployments

A deployment in Configuration Manager 2012 is the mechanism that associates applications and deployment types with a collection of devices or users so that the deployment may proceed. The deployment is not created as part of building the application and deployment type. Deployments are created by selecting the Deploy option from the ribbon when focused on a particular application in the console. Figure 8.10 shows the properties of a sample deployment. The process of building deployments will be detailed shortly.

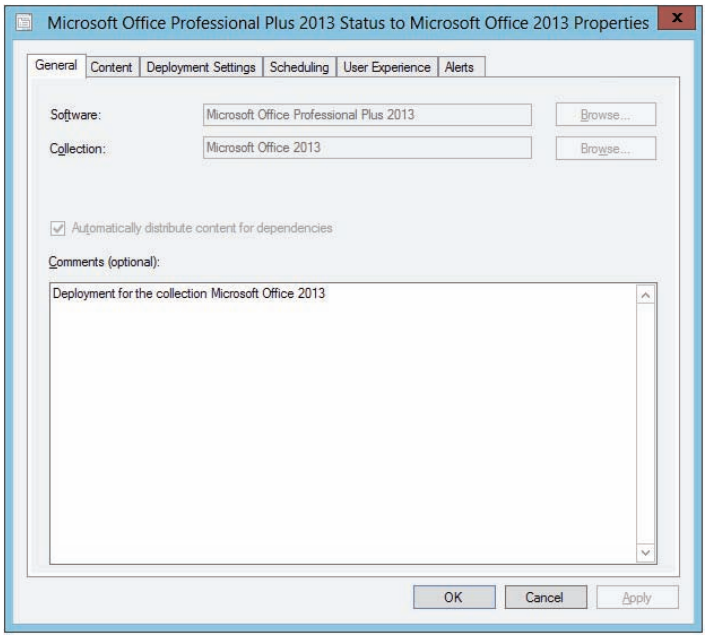


FIGURE 8.10
Sample deployment properties

The Application Deployment Process

The process of deploying applications in Configuration Manager 2012 has some similarity to previous versions but also has significant differences and additional options. One such example is the use of collections. It remains a requirement to have an application deployed to a collection in order for deployment to begin, but the use of collections is much changed from previous versions. In the past, application-specific collections of systems, and rarely users, would be created ahead of creating the package, program, and advertisement (classic Software Distribution terminology). The collections would be built according to specific criteria to define the scope of the distribution.

Configuration Manager 2012 Application Deployment introduces the concept of requirements. With requirements it is possible to define the rules of deployment within the deployment itself rather than build specific collections to do the same thing. When requirements are used instead of collections to specify deployment rules, the load of evaluation is effectively moved from the site server to individual client systems. Add to this that once a requirement rule is defined, it is retained and reusable for other deployments.

The use of requirements is optional, but they are both effective and efficient ways to validate deployment requirements. Administrators should consider strongly whether the old-style collection sprawl, which tends to junk up the console over time and can get fairly confusing to look at, really continues to be justified.

The best way to discuss the application deployment process is to create a sample application, deployment type, and deployment and then to demonstrate its execution in the environment. To start, a view of the Software Library ➢ Overview ➢ Application Management ➢ Applications node of the console is instructive.

Create Application Wizard

The Create Application Wizard creates an application and the first of potentially several deployment types. When you're getting started with Application Deployment in Configuration Manager 2012, the console will be not be populated with any deployments.

A Word about Packages

If you're migrating from Configuration Manager 2007, any packages are considered legacy (but still fully functional) in Configuration Manager 2012 and are migrated to the Packages node.

To get started with Application Deployment, you can either import an application from another Configuration Manager 2012 hierarchy by clicking the Import Application button or click Create Application. Both options are on the ribbon.

To build the sample application deployment, click Create Application to launch the Create Application Wizard. The general page of the Create Application Wizard is shown in Figure 8.11.

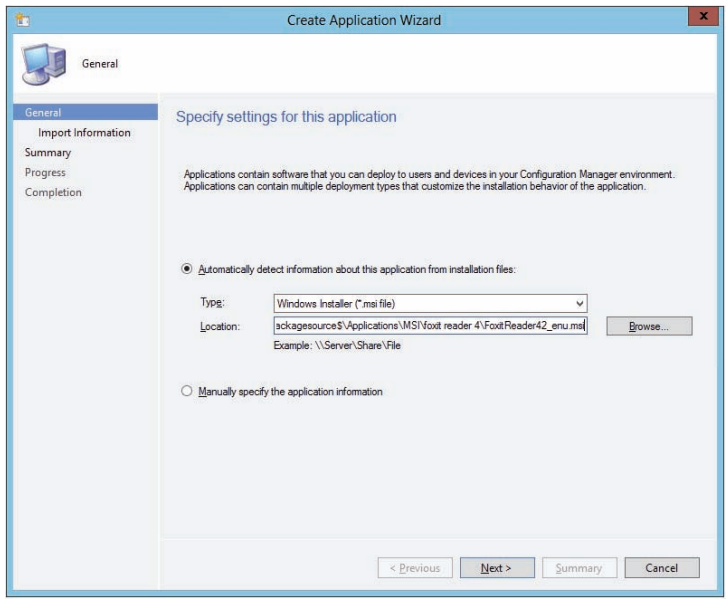


Figure 8.11
General page of the Create Application Wizard

The General page lets you choose either Automatically Detect Information About This Application From Installation Files or Manually Specify The Application Information. The quickest mechanism for configuring the sample application is to allow information to be automatically detected. This is particularly efficient when deploying an `.MSI` file. The option you choose on this page is dictated by preference and the type of application being defined. Using the option to manually define the information may be more appropriate depending on the type of content being deployed. Choosing this option simply requires manual entry of data that is otherwise supplied by the automatic option. In either case, reviewing all settings after they're initially configured with the wizard is a good idea.

For the sample application deployment, select the automatic option and choose Windows Installer (*.msi file) in the Type field. Then click Next to proceed to the Import Information page of the wizard, shown in Figure 8.12. This page of the wizard is displayed while information is being gathered from the specified source, in this case the `FoxitReader42_enu.MSI` file.

Once the Next option becomes available, click it to proceed to the General Information page of the wizard, shown in Figure 8.13.

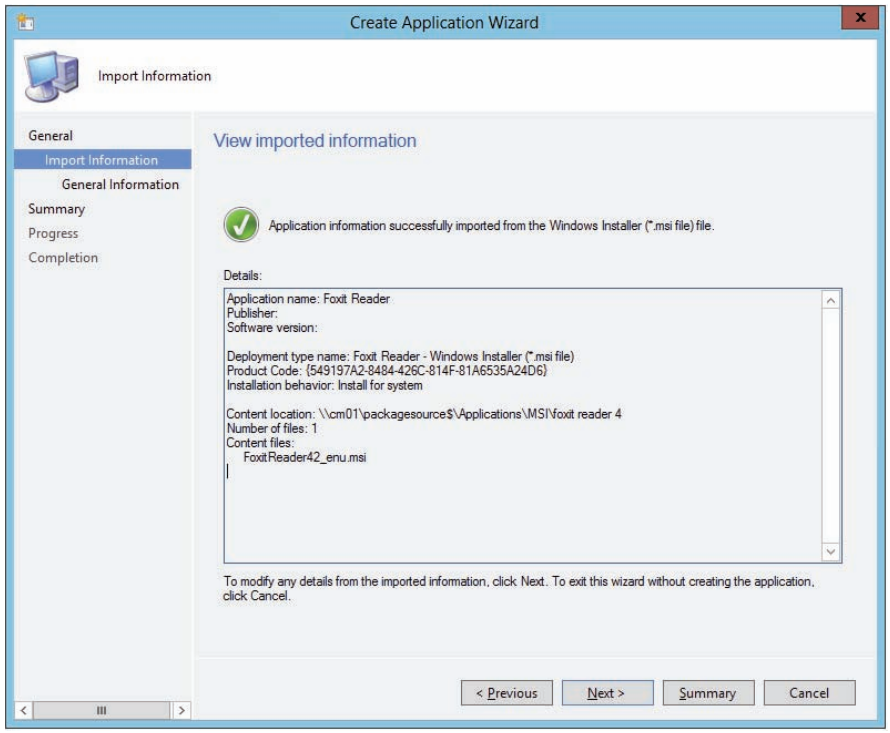


FIGURE 8.12
Import Information page of Create Application Wizard

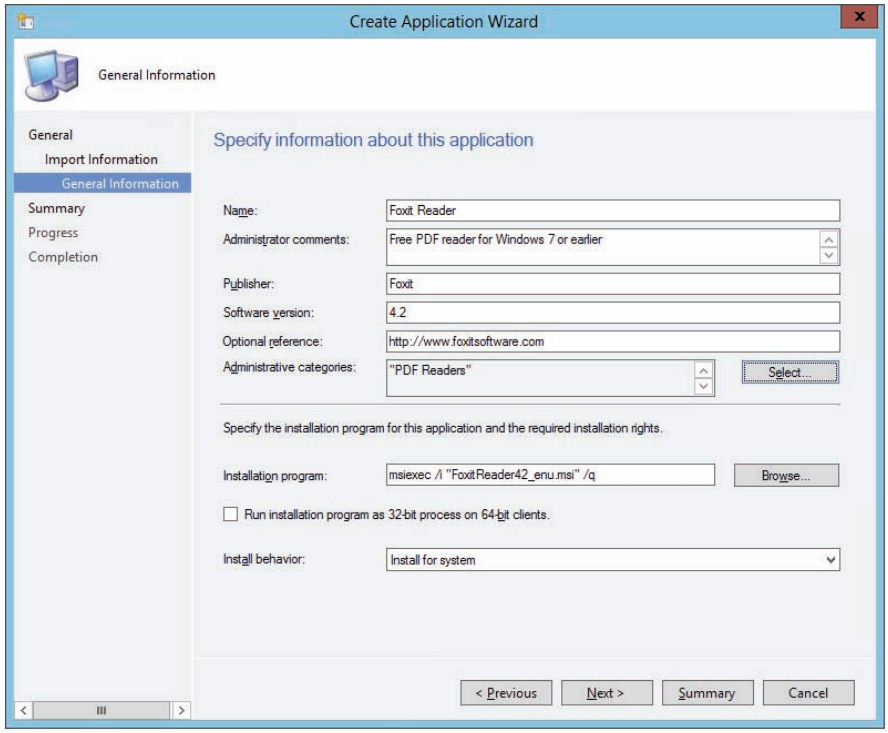


Figure 8.13
General Information page of Create Application Wizard

On the General Information page specify the requested information as follows:

Required Information The import process should have completed the required fields of the General Information page leaving only the optional fields to be completed.

Name The name of the application being created.

Installation Program The command line of the program to initiate application installation.

Install Behavior Options for this setting allow administrators to specify whether the deployment will be targeted to Install For User, Install For System, or Install For System If Resource Is Device, Otherwise Install For User.

Optional Information The information supplied as part of the optional fields is available for user review when applications are published in the Software Center or Application Catalog.

Administrator Comments Allows you to include any comments to further describe or detail the application.

Publisher Allows you to specify the software publisher.

Software Version Allows you to specify the software version.

Optional Reference Allows you to specify additional reference information for the application.

Administrative Categories Allows administrators to group applications together by user-defined categories that make sense in a given organization. Multiple categories may be specified.

There are two types of categories: administrative and user. The dialog here allows specification of administrative categories. Specifying user categories is done on the Catalog node of the application.

When you've finished entering information, click the Next button to proceed to the Summary page of the wizard. Review the summary information, and if it's correct, click Next to create the application. If errors are encountered, the wizard will display them. If the application is created successfully, exit the Create Application Wizard and return to the main console.

Creating an Application with PowerShell

Creating an application can be done also with the new PowerShell cmdlets. The workflow of creating an application with PowerShell consists of four steps:

1. Create the application.
2. Create a deployment type.
3. Distribute the content.
4. Deploy the created application.

In this example, we want to create an application called Google Chrome; it is located at the `packagesource$` share and will be deployed to the All Users collection.

Let's first create the application, by calling the `New-CMApplication` cmdlet:

```
New-CMApplication -name "Google Chrome" -Owner "Corporate IT" -Keyword
"Alternative Test Browser"

Add-CMDeploymentType -MsiInstaller -ApplicationName "Google Chrome"
-AutoIdentifyFromInstallationFile -InstallationFileLocation
"\\cm01\source$\Apps\MSI\Chrome\GoogleChromeStandaloneEnterprise.msi"
-ForceForUnknownPublisher $True

Start-CMContentDistribution -ApplicationName "Google Chrome"
-DistributionPointGroupName "All Content"

Start-CMApplicationDeployment -CollectionName "All Users" -Name
"Google Chrome" -DeployPurpose Available
```

Options for Application Deployment: the Ribbon

Now that an application is defined in the console, additional options appear on the ribbon. Let's take a quick pause to explore the options, as shown in Figure 8.14.

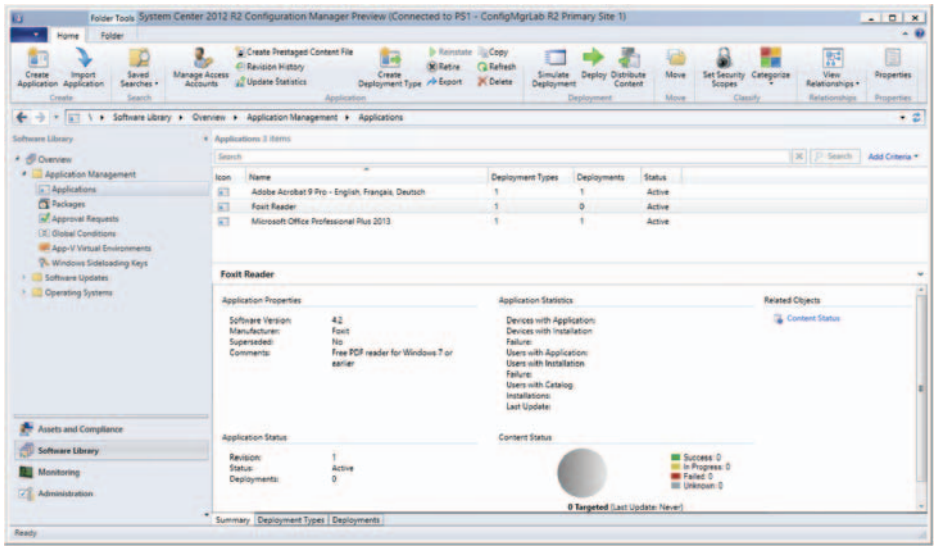


FIGURE 8.14
Ribbon options for application deployment

Wow, that's a lot of new options! Yes, and this is the first place that you start to see some of the new choices available for applications in Configuration Manager 2012.

Revision History The Revision History option tracks all changes that have been made to an application. This tracking not only creates a record of changes but also allows you to revert to a previous version if you've made a mistake. For the sample Foxit Reader application, we made a simple change to the administrator comments text, resulting in a new version being created. You can view the change by selecting the revision of interest, selecting the record, and clicking View. Notice in Figure 8.15 that the word *Microsoft* has been added to the administrator comments. If for some reason you don't want this change, you can simply pick the revision that is correct and click Restore to revert the application.

While this example is of a minor change, it does illustrate the power of revision tracking.

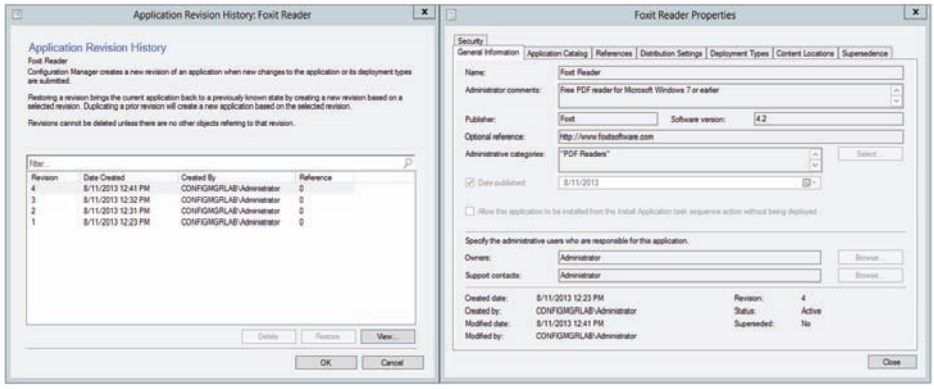


FIGURE 8.15
Viewing revision history

Create Prestaged Content File We've already discussed the challenges of managing distribution point content when replacing or adding distribution points in previous versions of Configuration Manager. The challenges are made worse when the distribution points are positioned across a slow or busy WAN connection from the site server. Historically, solutions for staging content in bulk without saturating such a WAN connection included utilities such as `preloadpkgonsite.exe`, scripts, or other third-party tools. But all of these tools came with their limitations and challenges. Configuration Manager 2012 introduces Prestaged Content as a mechanism to manage this type of scenario natively. When a distribution point supports Prestaged Content, administrators are able to choose applications that should be made available in a Prestaged Content file, along with all dependencies, which can then be copied locally onto the remote distribution point without the need for substantial WAN communication. Configuring Prestaged Content support requires setting the option on the distribution point and then using the Create Prestaged Content File Wizard to generate a file containing the content of interest. The Create Prestaged Content File Wizard is shown in Figure 8.16.

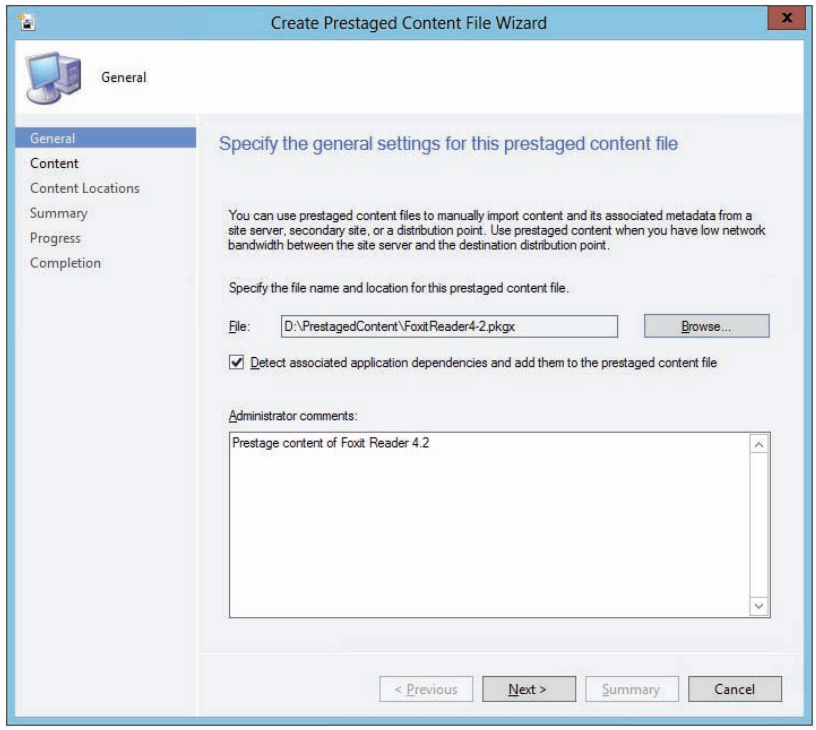


FIGURE 8.16 Create Prestaged Content File Wizard

Create Deployment Type A deployment type for the sample Foxit Reader application has already been created by the Create Application Wizard. We'll review this shortly. For a given application it is possible to create multiple deployment types. Selecting this button from the ribbon launches a wizard that walks through the configurations needed for creating new deployment types to augment deployment of the selected application.

Retire/Reinstate The option to retire an application allows administrators to effectively mark an application as no longer deployable without deleting it from the console. There are a couple of advantages to this approach:

- The application deployment status is not removed.
- If questions arise about the application configuration, the configuration may easily be reviewed.
- If it becomes necessary to reinstate the application to an active status, it is possible to do so by simply selecting the Reinstate option.

Delete It is pretty obvious what this option does but it's still worth a bit of discussion. As you will see shortly, it is possible (and likely) that applications will be tied to each other through dependencies and supersedence relationships. When these relationships exist, or when there is a deployment defined for an application, the deletion option will fail to work. This prevents potentially removing an application that is critical to the function of another. While this is good, it is important to understand and be able to resolve these relationships. The View Relationships option helps detail all configured links for a given application.

Simulate Deployment This is a really cool option in Configuration Manager 2012 that allows administrators to perform a test deployment of a configured application that will function only to validate associated relationships and report back on what kind of success might be expected. The Simulate Application Deployment Wizard is shown in Figure 8.17.

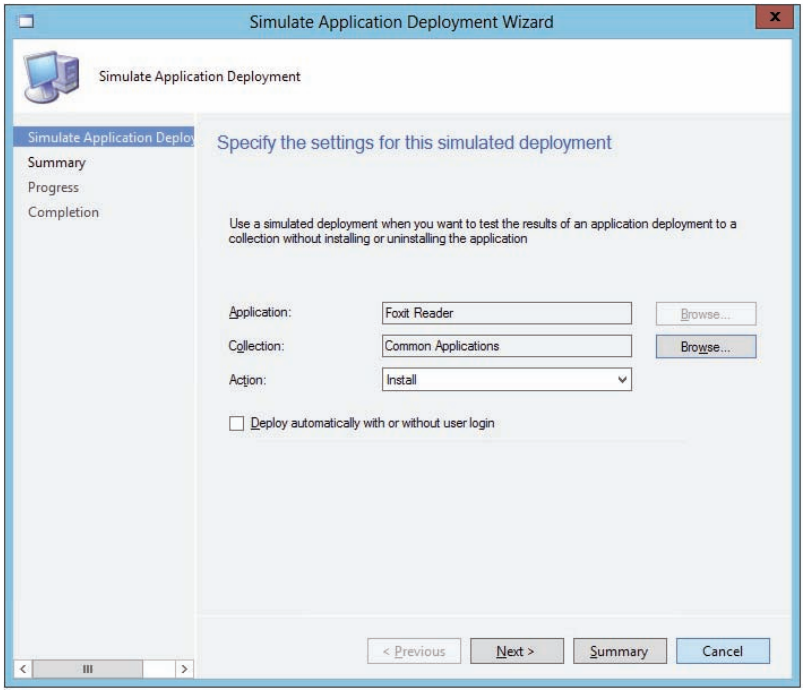


FIGURE 8.17
Simulate Application Deployment Wizard

Export A welcome addition to Configuration Manager 2012 is the ability to share almost any configuration, including application definitions, between Configuration Manager 2012 hierarchies if you do not want to use the migration feature. The Export button on the ribbon launches a wizard to walk through steps to complete the export. The wizard is shown in Figure 8.18.

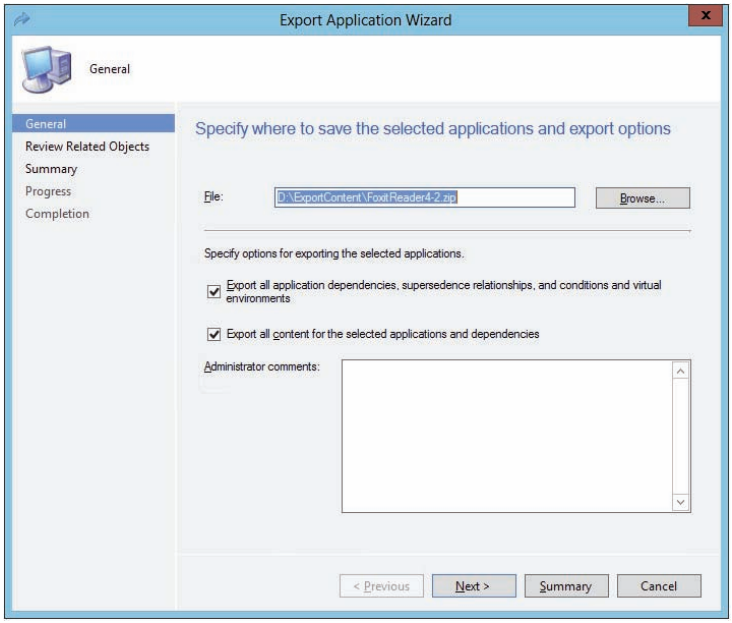


FIGURE 8.18
Foxit Reader 4.2 properties in the General tab of the Export Application Wizard

The content created by the Export Application Wizard is available for import into another Configuration Manager 2012 hierarchy using the Import Application button from the ribbon.

Another potentially interesting use of this functionality is as an extra level of backup for data configured in the site. Consider retiring an application as an example. It could be that the application is ready to be purged from the console, but you would like to keep a copy around for those scenarios where it might be needed again. Exporting before deletion is the perfect answer!

Deploy Creating an application and associated deployment type(s) does not result in any action taking place. To trigger action a deployment is needed. Deployments are *not* created as part of the Create Application Wizard and must be configured through the Deploy Wizard, as will be shown for the Foxit Reader sample application shortly.

Distribute Content Deploying applications requires that content needed for the application be distributed to target systems/users. To make content available to clients it must be staged on a distribution point. We'll review the options to distribute content for the Foxit Reader sample application shortly.

At this stage we will just say that while this option is useful to stage content to distribution points, using it isn't strictly required. By defining distribution point groups to include collection mappings, when a collection is targeted with a deployment the content needed will automatically deploy to the defined distribution points—a nice option to save a couple of extra mouse clicks!

Move This option allows administrators to move applications between defined folders. This helps keep things organized as the number of defined applications increases.

Set Security Scope Security scopes are more of a topic for security, covered in detail in Chapter 17. The role security scopes play with applications is interesting, though, and merits a brief discussion.

A significant change in Configuration Manager 2012 is in how security is handled, both in terms of assignment of user roles and the ability to mark certain objects, such as applications, as being part of one or more defined security scopes. Configuration Manager 2012 console users may also be assigned to one or more security scopes; by so doing, you limit the users' visibility of the Configuration Manager 2012 environment, including applications, to just those items that are part of their assigned scope(s).

Categorize As already noted when creating the sample Foxit Reader application, it is possible to create and assign categories to applications for the purposes of organization or grouping. Managing categories can be done as part of the application creation, but that is cumbersome, so the Categorize option on the ribbon is available to enable easier category management.

Properties This option will open the Properties dialog for selected objects in the console and is useful for editing settings made through the various wizards.

Exploring the Sample Application

The wizard operations are complete. The result? An application and an associated deployment type. That was easy! But what options did the wizard actually set for these items, and what options are available? To take a look, select the application, and from the ribbon, select Properties. The Foxit Reader 4.2 application property screen opens to the General Information tab, as shown in Figure 8.19.

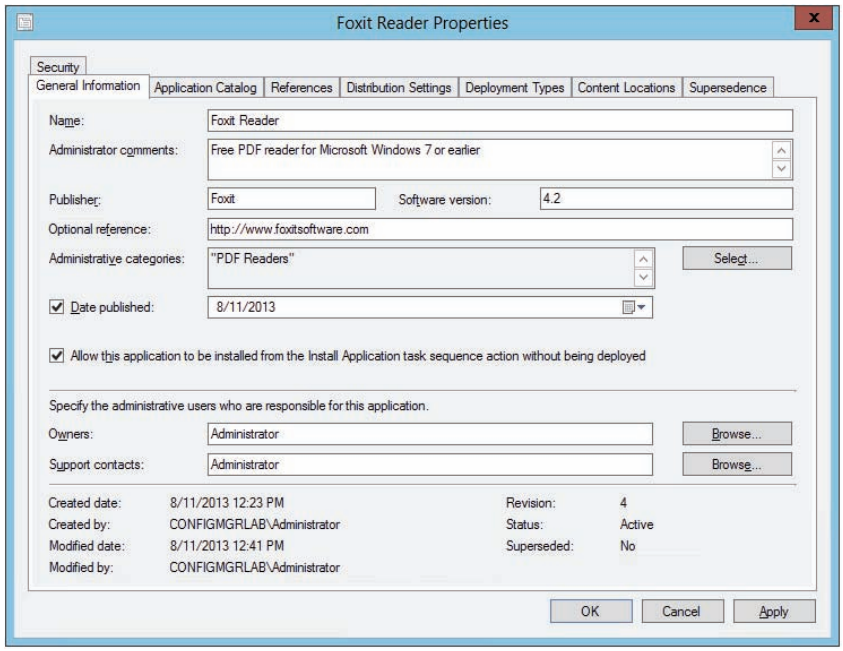


FIGURE 8.19
Foxit Reader 4.2 Properties—General Information tab

Most of the options on the General Information tab have already been discussed. In addition to those already mentioned, a few additional options are available:

Date Published The published date allows administrators to note when the application was published. This date defaults to the current date if not selected and modified.

Allow This Application To Be Installed From The Install Application Task Sequence Action Without Being Deployed This option is not selected by default. If the application should be deployable via a task sequence, you must select this box. If the option isn't selected, the task sequence will fail, or you will not be able to select the application while creating a new task sequence.

Owners This option allows administrators to define who the owner is for the given application. This information is then displayed in Software Center and also in the Application Catalog.

Support Contacts This option allows administrators to define who users should contact if problems are encountered with the application. This information is then displayed in Software Center and also in the Application Catalog. The Browse button allows you to select users from Active Directory if desired, or you may enter users manually.

The bottom section of the General tab provides summary information for the application, including its status, whether it is superseded by another application, and the current revision number.

Selecting the Application Catalog tab details options related to publishing the application in the Application Catalog. Some options here will be provided already. If you're publishing in the catalog, you'll likely need to modify or supply some of the default options. Remember, publishing in the Application Catalog is not actually accomplished on this tab. Rather, this tab collects information to be used *if* the application is published in the catalog. Associating your deployment, described soon, with a collection of users or user groups will result in the application showing up in the catalog. Options for the Foxit Reader sample are shown in Figure 8.20.

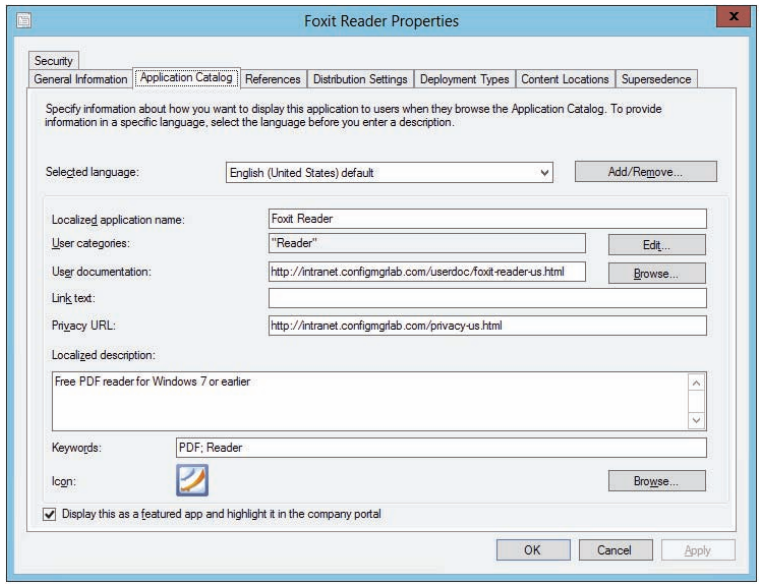


FIGURE 8.20
Foxit Reader 4.2 Properties—Application Catalog tab

Selected Language This option allows administrators to add or remove languages that should be supported by the application in the catalog and also to specify which language should be displayed.

Localized Application Name This option presents the application name localized by the current language selected.

User Categories User-targeted applications and device-targeted applications maintain separate category lists for grouping purposes. If publishing this application for users, administrators have the option to select an existing user category for describing the application or to create a new one.

User Documentation With this option, administrators are allowed to specify a path that is available to the user for additional information on the application. This path may be a web page that the user might visit or a link to an online document.

Link Text This option allows administrators to specify what specific text is displayed in the catalog instructing users how to obtain additional documentation.

Privacy URL An application can have a privacy policy. As an administrator, you can configure the URL that redirects you to the website with the privacy policy.

Localized Description This section allows users to specify text, localized to the language selected, to be displayed as the application description in the catalog.

Keywords When multiple applications and categories are present in the catalog, locating specific content may be difficult. To help with the location process, administrators have the option to specify search keywords for an application that will aid users in finding its location.

Icon Administrators can choose from a substantial list of custom icons that might be associated with the application.

Display This As A Featured App And Highlight It In The Company Portal An application can be configured as a featured app in the company portal.

Selecting the References tab will display any other defined applications that either depend on the one being configured or any applications that supersede the one being configured. Also, depended virtual environments, if available, are displayed on the References tab. In the case of the sample Foxit Reader application, no dependency or superseding application is defined.

The next tab is the Distribution Settings tab; here you can configure the distribution settings for the application. Configure the distribution priority or the prestaged distribution point settings.

The Deployment Types tab, as shown in Figure 8.21, lists all defined deployment types for the application. It is possible to configure multiple deployment types to cover all potential deployment scenarios for the application. Deployment types will be discussed in detail shortly.

The Content Locations tab, as shown in Figure 8.22, will list all distribution points or distribution point groups that have been configured to host the content. In the sample Foxit Reader application, distribution points have not yet been defined but will be shortly. If they are defined, this tab allows you to validate, redistribute, or remove the content from the distribution points or distribution point groups.

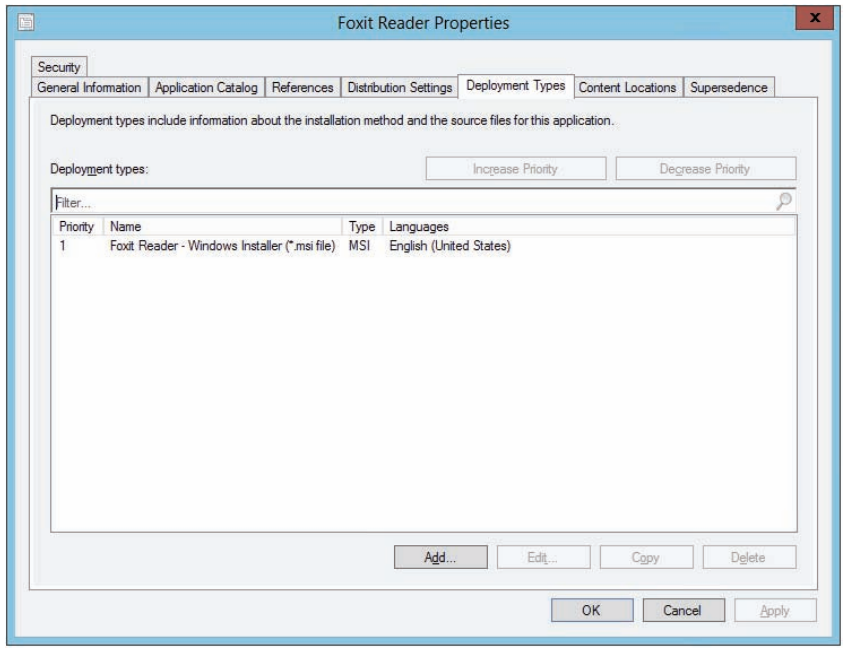


FIGURE 8.21
Foxit Reader 4.2 Properties—Deployment Types tab

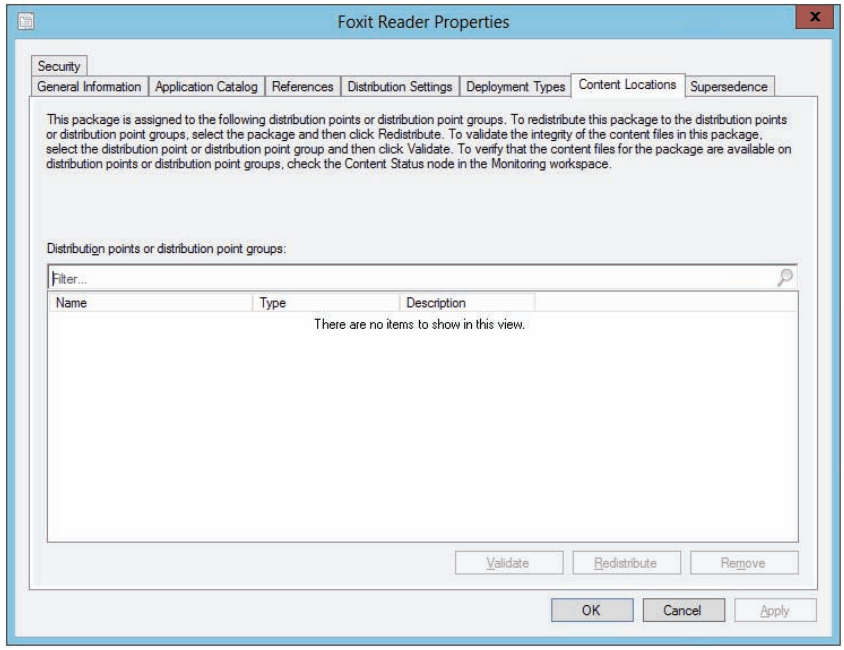


FIGURE 8.22
Foxit Reader 4.2 Properties—Content Locations tab

The Supersedence tab, as shown in Figure 8.23, lists any application that the current one supersedes. The ability to build links between applications that supersede each other is much like the experience that is seen with patches and brings significant benefit. (This is discussed in detail in the section "Supersedence" later in this chapter.) The sample Foxit Reader application does not currently have any superseding relationships defined. By clicking Add on this page it is possible to define the application that is superseded by the one being configured and also to specify the new deployment type to use and whether the previous application should be uninstalled prior to installing the current version. This allows administrators great flexibility in controlling how deployments take place, especially when upgrading from previous versions.

The Security tab allows administrators to specify users who may access the application and their effective rights to the application.

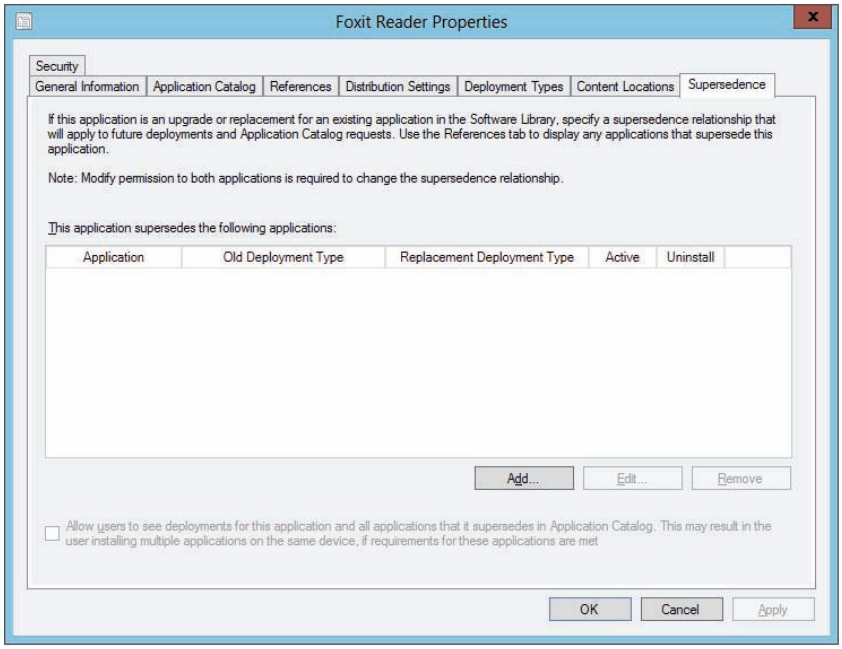


Figure 8.23
Foxit Reader 4.2 Properties—Supersedence tab

Exploring the Deployment Type

In addition to creating the sample application, the Create Application Wizard also created one deployment type. This was already noted briefly and is shown in Figure 8.21.

The current sample application has only a single deployment type configured. This is shown in Figure 8.24. Note from this same figure that deployment types have as part of their definition an assigned priority. When multiple deployment types are present, it is possible to rank how they should be evaluated in relationship to each other using the Priority option. The priority for a deployment type may be increased or decreased from either the context menu brought up by right-clicking the deployment type or from the Deployment Type option on the ribbon, which is also identified in Figure 8.24.

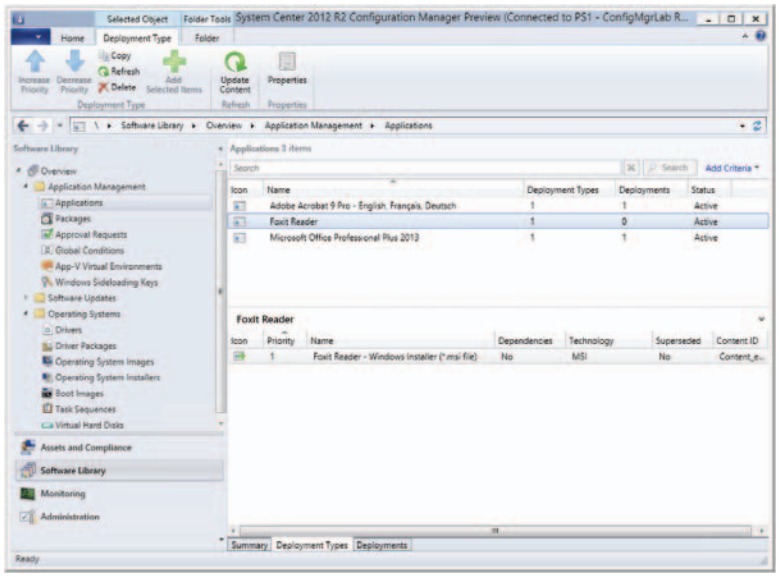


FIGURE 8.24
Displaying deployment type properties

There are several options when creating a deployment type. To access the sample deployment type, either navigate to it through the properties of the application and click Edit, or simply select the sample Foxit Reader application, and in the bottom of the screen select the Deployment Types tab. This is also shown in Figure 8.24. Right-click the only deployment type available and select Properties.

Selecting Properties will display the properties for the deployment type with the General tab showing, as shown in Figure 8.25. All of the information displayed on the General tab except for the Administrator Comments text was supplied by the Create Application Wizard.

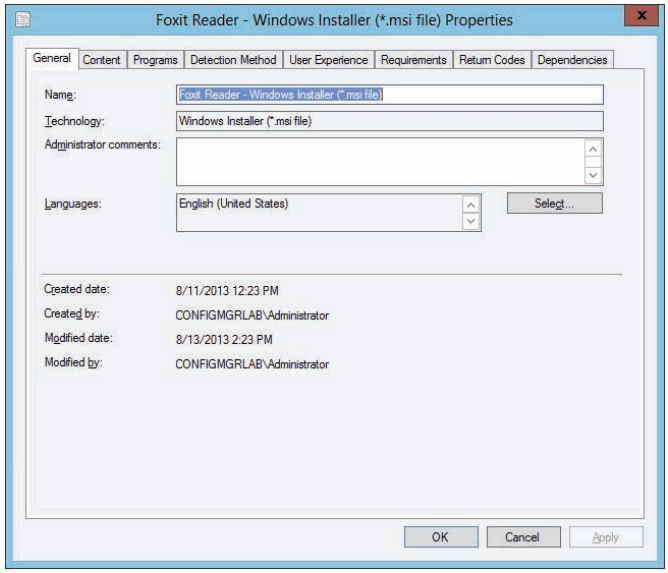


FIGURE 8.25
Sample deployment type properties—General tab

Name This is the name of the deployment type. Supplying a descriptive name for each deployment type helps administrators know the intended use of each deployment type configured.

Technology This describes what type of item is being deployed and will change based on whether an MSI (as in this case), script, or executable is being deployed.

Administrator Comments This field allows administrators to provide any needed additional information regarding the deployment type.

Languages This field allows administrators to optionally select the specific language for the deployment type.

The bottom section of the General tab provides additional information as to the creation and modified dates for the deployment type.

Selecting the Content tab of the deployment type properties, as shown in Figure 8.26, will list various options specific to configuring content.

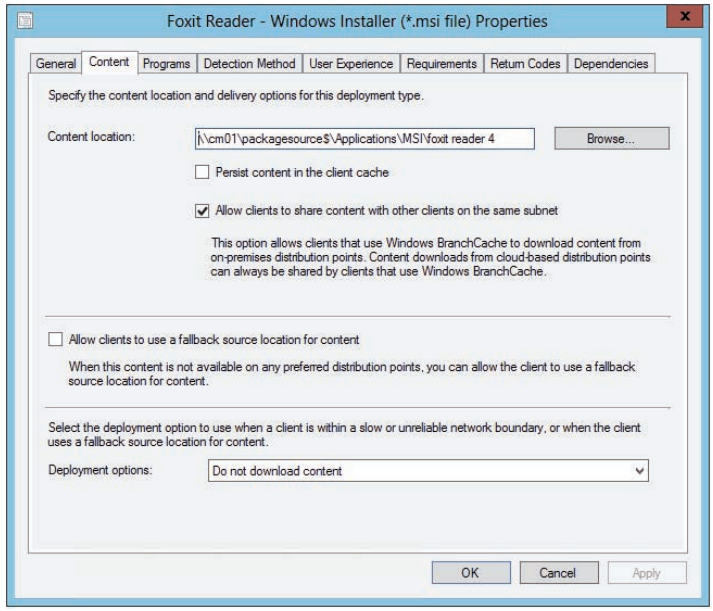


FIGURE 8.26
Sample deployment type properties—Content tab

Content Location The Content Location option allows administrators to specify the location on the network where Configuration Manager 2012 can find the content to be deployed. The path listed for this option must be specified in UNC format.

Persist Content In The Client Cache This option, disabled by default, flags that the content being deployed should remain in the client cache rather than being marked eligible for deletion. You should consider this option if the content being deployed will be reused. An example might be a script that runs periodically against clients. In such a case it is more efficient and predictable to persist the script in the client cache so it is available locally each time it is scheduled to run. If this option is not selected, after the script content runs successfully the first time, it will be eligible for deletion from the client cache if space is needed and will need to be downloaded again at the next runtime.

Allow Clients To Share Content With Other Clients On The Same Subnet This option, enabled by default, allows clients (Windows Vista and higher) on the network segment to leverage BranchCache capabilities of the operating system and act as a location cache for content that other clients on the same network segment may need. When a local peer client is detected that already has content available, clients needing the content will simply download it locally rather than from a distribution point.

There are multiple scenarios where this type of configuration is helpful. Consider the following:

- Clients reside in a small office with no local distribution point and limited bandwidth. When applications are configured to support shared content, when a single client in the office has downloaded the content, either in total or in part, then it will be possible for other clients in the same office to access the content locally rather than traversing the network.
- Clients reside in a small office with a local distribution point hosted on a workstation system and limited bandwidth. In this scenario a local distribution point exists. Depending on the total number of workstations acting as distribution points and the total number of clients, it may still be useful to enable shared content distribution. When a distribution point is configured on a workstation, there is a limit of 20 simultaneous connections possible. If this small office had 100 Configuration Manager clients all needing to run an application at the same time, connections to the distribution point may be exceeded. Having content persisted in the cache of various client systems would present another option for content download.

When an administrator is planning the Configuration Manager 2012 implementation, having the ability to factor in shared content distribution as an option may allow fewer distribution points to be installed at a given location.

Allow Clients To Use A Fallback Source Location For Content. In Configuration Manager 2012 and with the introduction of boundary groups, protected distribution points will be common. When clients are connected to the corporate network directly, and if Configuration Manager 2012 distribution point access is properly configured, there should be little problem finding a distribution point that is available for use. If a client connects remotely from a boundary not configured in Configuration Manager boundary groups, the client may not be able to find a distribution point that is accessible to it because of boundaries. Setting this option, disabled by default, to allow those clients to communicate with an unprotected distribution point is important to successful application deployment. It probably goes without saying, but to be clear, setting this option by itself is only part of the equation. Distribution points themselves must be configured to be used for fallback, which is not enabled by default.

Deployment Options When configuring boundary groups in Configuration Manager 2012, administrators are able to designate each included distribution point that is part of the boundary group as being across either a fast or slow connection. This option allows administrators to define how application deployment will proceed. The default option is Do Not Download Content, which means the client will delay content download until it moves inside a boundary noted as being fast. The other option is Download Content From Distribution Point And Run Locally, which will allow content to be downloaded regardless of connection quality. Remember that clients attempt to download content using BITS, which works to ensure transfers complete successfully, even across unreliable or slow network conditions.

The Programs tab of the deployment type properties, as shown in Figure 8.27, lists program installation and uninstallation options.

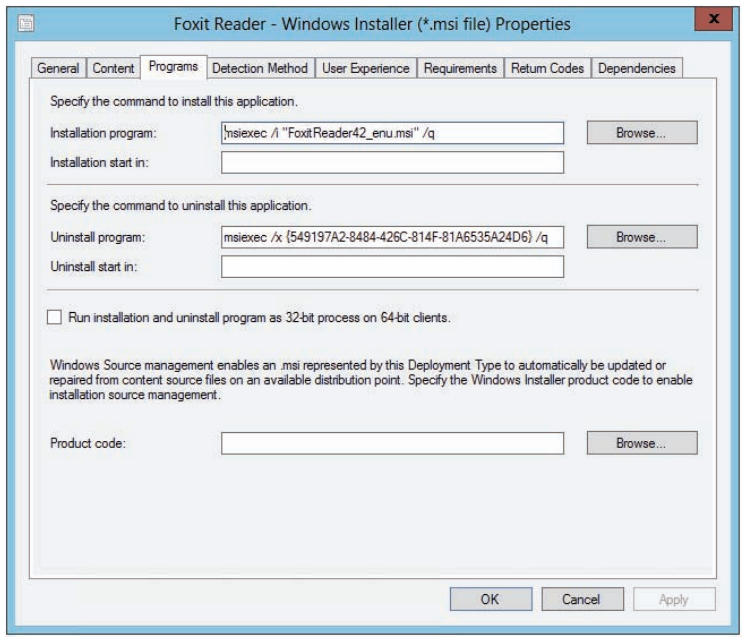


Figure 8.27
Sample deployment type properties—Programs tab

Installation Program This option allows administrators to specify the command line to be used for program installation. This command line will be initiated from the source content downloaded from the distribution point, as specified earlier.

Installation Start In This option allows administrators to specify a specific directory that installation should be initiated from. This option is useful when the root of the content folder on the distribution point does not contain the files needed to initiate an installation. In such a case it would be possible to specify which folder within the content does contain the needed information.

Uninstall Program This option allows administrators to specify a command that is useful to uninstall the given application. If you're using an MSI, as in the example, the uninstall command is straightforward. It would also be possible to include a script to automate removal of any type of application install.

Uninstall Start In This option is the same as for Installation Start In discussed previously.

Run Installation And Uninstall Programs In 32-bit Process On 64-bit Clients This option allows administrators to toggle that 32-bit applications should be handled within their own 32-bit process when running on a 64-bit system.

Product Code This option is specifically for use when deploying MSI applications. The design of MSIs allows for application self-repair and also installation of additional features if the application user selects functions that require them. In order for MSIs to work properly, they must be configured to know where the original source files are located. This option serves that purpose.

Selecting the Detection Method tab of the deployment type's properties, as shown in Figure 8.28, lets you see options for use in detecting whether an application being deployed is already present on the target device.

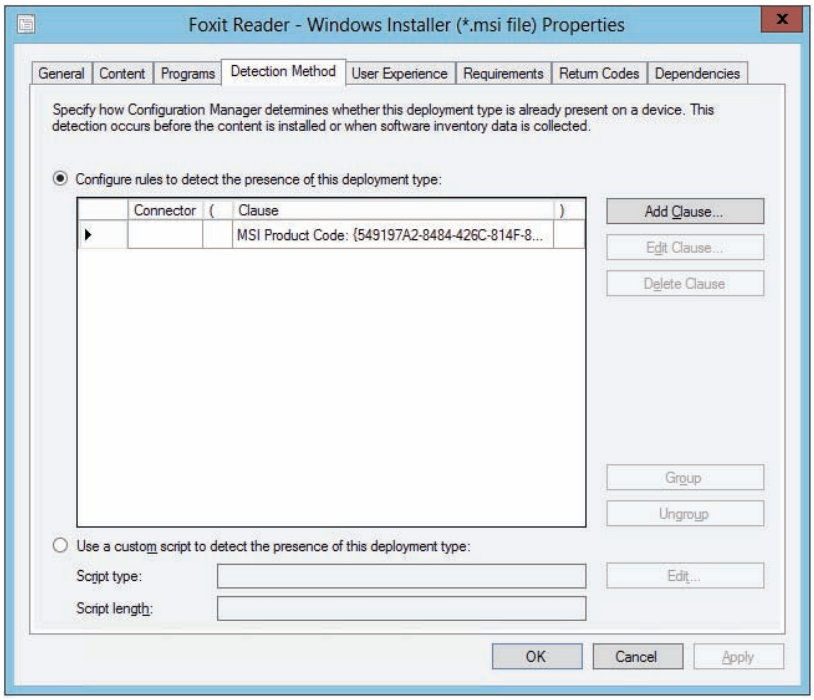


FIGURE 8.28
Sample deployment type properties—Detection Method tab

A new feature for application deployment in Configuration Manager 2012 is the ability to configure detection logic to determine if an application is already present on the target device before simply installing it again. This option is much like what is already part of software update deployment but has been brought into the Application Deployment feature. Properly configuring this option will avoid application reinstallations and is also pivotal to verifying dependencies and other configured relationships. When you're using an MSI, as in the example Foxit Reader application, this information is supplied automatically and is straightforward. Regardless of the type of application being installed, it is possible to configure a useful detection mechanism. Clicking Add Clause opens the Detection Rule dialog box, which is used to add criteria needed to detect if the application is already installed. We'll more fully explore this wizard later in the chapter. Also note the option to execute a custom script to detect an already installed application. In most cases, the available options for detection will suffice, but if not, the script option allows almost any scenario for detection to be handled.

The User Experience tab of the deployment type's properties, as shown in Figure 8.29, lists options that allow administrators to define the experience users will have during application deployment.

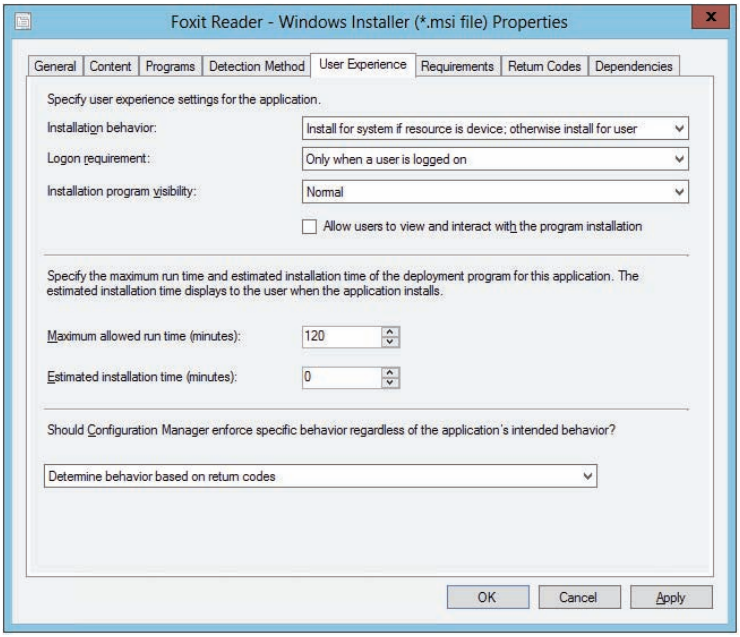


Figure 8.29
Sample deployment type's properties—User Experience tab

Installation Behavior This option allows administrators to define whether the application will be a deployment for a system or for a user. A third choice allows administrators to define the deployment for a system if the resource is a device but for a user otherwise. Selecting a deployment to a user will gray out the next option so that a deployment can only be executed when a user is logged on.

When a deployment is configured for a system, this indicates that the deployment will take place under the security context of the local system account. When a deployment is configured for a user, this indicates the deployment will take place under the security context of the logged-on user.

Logon Requirement This option allows administrators to configure whether a user needs to be present during a deployment or not. When a deployment is identified as being for a user, this option is gray. When a deployment is identified as being for a system, there are three available choices:

Only When A User Is Logged On This option requires a user to be logged onto the client system before a deployment will proceed, even when the deployment is identified as being for a system.

Whether Or Not A User Is Logged On This is by far the most commonly used option because it allows a deployment to proceed without the user being present.

Only When No User Is Logged On This option ensures no application deployment takes place when a user is logged onto the system. This option would be very useful in a scenario where it is crucial to ensure users are not disrupted for application deployment, such as when a retail kiosk system is in use by a customer.

Installation Program Visibility Options here allow administrators to configure whether the program will run Maximized, Normal, Minimized, or Hidden. The default option is Hidden. Ultimately these choices really only come into play if an application is deployed to a user or to a system and the option Allow Users To View And Interact With The Program Installation is chosen. Deployments targeted to a system execute in the context of the local system account, so without that option, users wouldn't be aware of any information displayed on the screen during installation since it is not happening in their logged-on context.

Allow Users To View And Interact With The Program Installation This option, only available when Only When A User Is Logged On is selected for the Logon Requirement, is enabled by default and cannot be disabled when the installation is identified as being for a user, but it can also be enabled when the installation is identified as being for a system.

User When an application is being deployed to a user, the installation proceeds under that user's credentials, and thus the user is able to interact with the application unless it is being deployed silently.

System When the application is being deployed to a system, the installation proceeds under the local system's credentials. Since the user's credentials aren't in use, this effectively hides any interaction from the user. Setting the option to Allow Users To View And Interact With The Program Installation causes the system to pass the local system's interactive experience through to the logged-on user. While this option is not often used in production environments, it can be a useful troubleshooting option so that administrators are able to watch an application as it installs and identify any problems that might occur.

Maximum Allowed Run Time (Minutes) This option allows administrators to configure a maximum amount of time that an application install is able to run before being forcibly terminated. Typically the default setting of 120 minutes is more than sufficient, but in some cases application deployment errors may cause a deployment to appear hung, which will cause the installation to run past the configured window and be terminated. An example of such a situation would be if the application requires user input but is hidden from the user either because of the settings just discussed or because the application was set to run silently. In such cases, using the option Allow Users To View And Interact With The Program Installation would help identify the problem.

In many environments administrators didn't think to adjust this setting, and in many cases this presented no issue. With the introduction of maintenance windows in Configuration Manager 2007, however, this setting took on great importance. If maintenance windows are defined for the environment, the Configuration Manager client will first check to see if it is in a maintenance window before attempting to execute the application. If the client is within a maintenance window, then the amount of time configured for the install (this setting) will be compared against the time remaining in the maintenance window. If insufficient time remains, the application deployment is canceled and attempted at the next opportunity. From this alone it is clear that configuring a realistic value for this setting is critical when making use of maintenance windows in the environment.

Estimated Installation Time (Minutes) This option allows administrators to specify how long they anticipate that an application will take, at most, to complete the install. This setting has been an option in previous versions of Configuration Manager.

The bottom part of the User Experience tab allows administrators to configure how the Configuration Manager 2012 client should respond after the application deployment is complete. There are four options available:

Determine Behavior Based On Return Codes This is the default option and likely makes the most sense in most scenarios. When this option is selected, the action taken by the Configuration Manager 2012 client will be determined by application return codes. Some return codes indicate that the application was successful, while others indicate the application was successful but requires a reboot. Still others may indicate some sort of failure. Administrators are able to specify custom return codes, discussed next, for applications that do not adhere to standards.

No Specific Action This option simply allows the Configuration Manager 2012 client to exit after the application install is complete, without any further action.

The Software Install Program Might Force A Device Restart This option indicates to the Configuration Manager 2012 client that once the application deployment completes, the application itself will force a reboot if necessary.

Configuration Manager Client Will Force A Mandatory Device Restart This option causes the Configuration Manager 2012 client to force the device to reboot following an application installation.

Selecting the Requirements tab of the deployment type's properties, as shown in Figure 8.30, lists options that administrators can use to define requirements that must be met before the application installation is attempted. This page is a starting point, allowing administrators to review requirements already configured or add additional requirements.

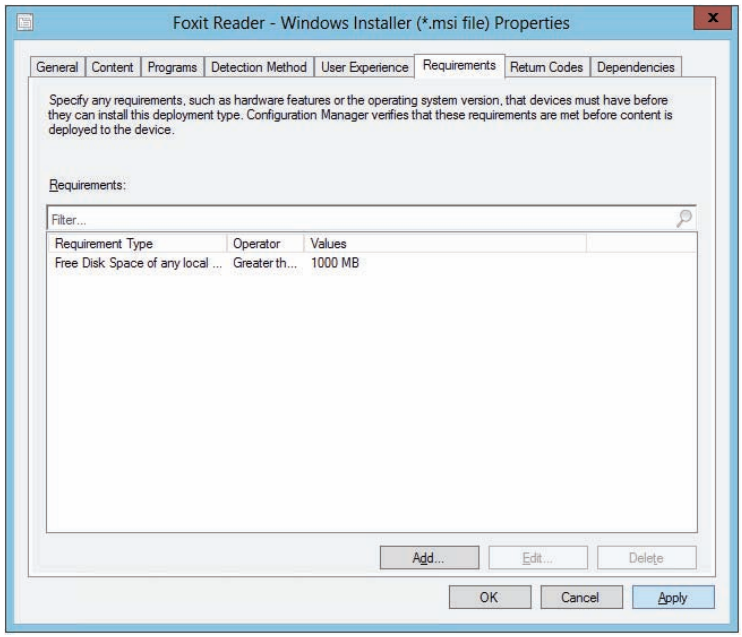


Figure 8.30
Sample deployment type's properties—Requirements tab

The addition of deployment rules is a significant modification in Configuration Manager 2012 and will be detailed later in the chapter. For now, suffice it to say that rules are intended to either take the place of building unique collections with criteria per deployment that need to be managed by the site server or move the responsibility for rules checking to the client system instead. This practice will allow administrators to shift their thinking about how many collections they need to maintain, but they will need some learning time to fully acclimate to this change!

Selecting the Return Codes tab of the deployment type's properties, as shown in Figure 8.31, allows administrators to define possible return codes for the application and how they should be interpreted by the Configuration Manager 2012 client. The default values are shown in the figure. Administrators choose whether the default values are sufficient or they need to augment them.

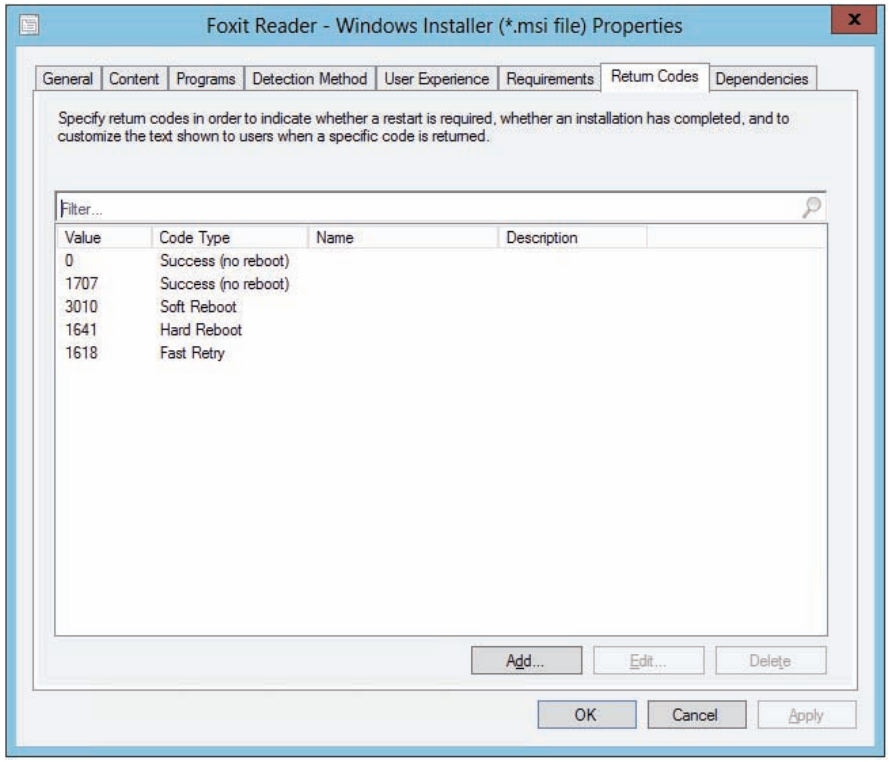


FIGURE 8.31
Sample deployment type's properties—Return Codes tab

In most cases, the default return codes will be sufficient, but in some cases, applications introduce their own return codes in an effort to help identify certain conditions that may exist at deployment time. A return code of 1, for example, may indicate a successful deployment but one that needs some sort of post-deployment action. If a return code of 1 was not added to this list, then the Configuration Manager 2012 client would interpret it as a failed deployment.

Selecting the Dependencies tab of the deployment type's properties, as shown in Figure 8.32, allows administrators to define any software items that must be installed prior to the current application being installed.

Dependencies will be detailed later in the chapter, but a quick look at the column headers reveals that along with specifying dependencies, administrators are also able to specify whether a given dependency, if absent, should be automatically installed as part of the application deployment.

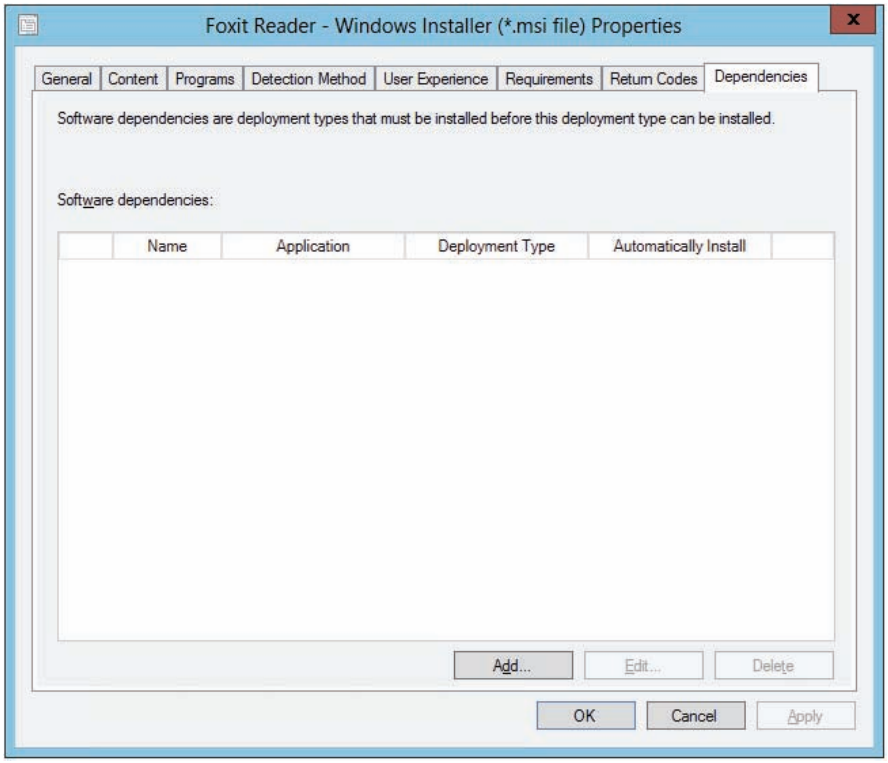


Figure 8.32
Sample deployment type's properties—Dependencies tab

Create Deployment Wizard

The Create Application Wizard worked to build the sample Foxit Reader application and deployment type but did nothing to build an actual deployment. To build the deployment, click Deploy from the ribbon to launch the Deploy Software Wizard. The General page of the Deploy Software Wizard is shown in Figure 8.33.

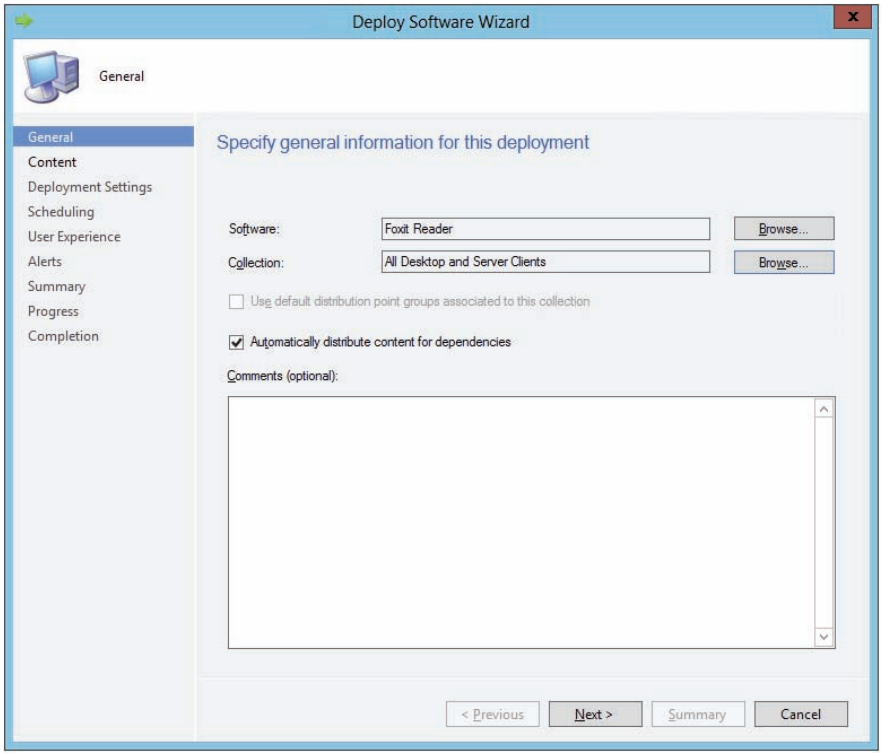


FIGURE 8.33 Deploy Software Wizard—General page

Software On the General page of the Deploy Software Wizard the software to be deployed likely is already specified, in this case Foxit Reader 4.2. If the provided selection is incorrect or is missing, clicking the Browse button will allow you to select the correct application.

Collection A deployment must be associated with a collection. A collection is a group of devices or users where the deployment should be made available. Administrators familiar with previous versions of Configuration Manager are accustomed to building collections specific to a given deployment. This can still be done in Configuration Manager 2012, or it is possible to target a generic collection and rely on the requirement rules, mentioned earlier and discussed in more detail later in this chapter, to determine which systems actually run the deployment. In practice, a hybrid approach will likely be used, where a collection is built containing systems that should be targeted with an application but without the various deployment criteria such as minimum disk space, minimum processor, minimum software version, and so on. These latter options will be managed as part of the application's Requirements settings.

Use Default Distribution Point Groups Associated To This Collection In Configuration Manager 2012 it is possible to associate collections with a distribution point group. If this is done, the option shown would be available for selection and would result in the deployment being automatically distributed to distribution points based on collections chosen.

The benefit of being able to link a collection with a distribution point group allows administrators additional flexibility. As an example, it would be possible to build collections per machine type per a given geography or office location. Then, when building distribution groups, the relevant collections and distribution points that serve those collections could be grouped together, facilitating more efficient management.

Automatically Distribute Content For Dependencies If dependencies are defined for an application and if those dependencies have not been deployed to the distribution points selected for the deployment being configured, selecting this option will ensure that the content for the dependency is made available in the event it is needed.

Comments The Comments section allows administrators to optionally add any information that may be pertinent for the deployment.

The Content page is shown in Figure 8.34. On the Content page, administrators are able to view currently assigned distribution points and distribution point groups. If the content is not already on any of the distribution points, you can add the content to distribution points or distribution point groups. You can also select additional distribution points or distribution point groups that are appropriate locations to stage the content for client access.

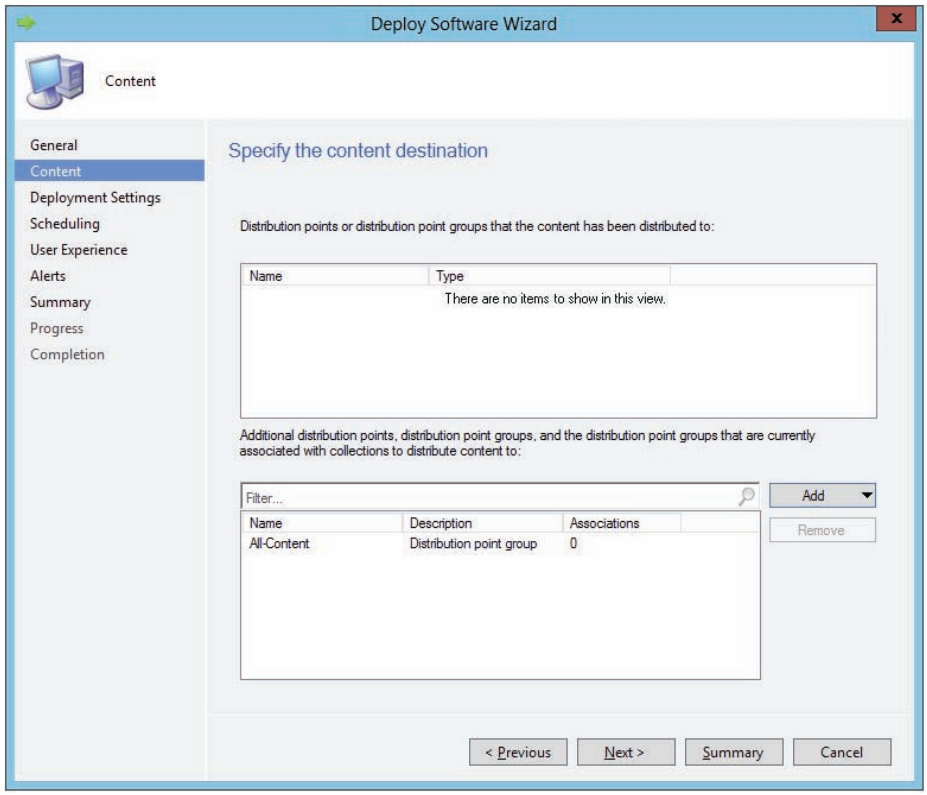


FIGURE 8.34 Deploy Software Wizard—Content page

When you've finished with the settings on the Content page, click Next to continue to the Deployment Settings page, as shown in Figure 8.35.

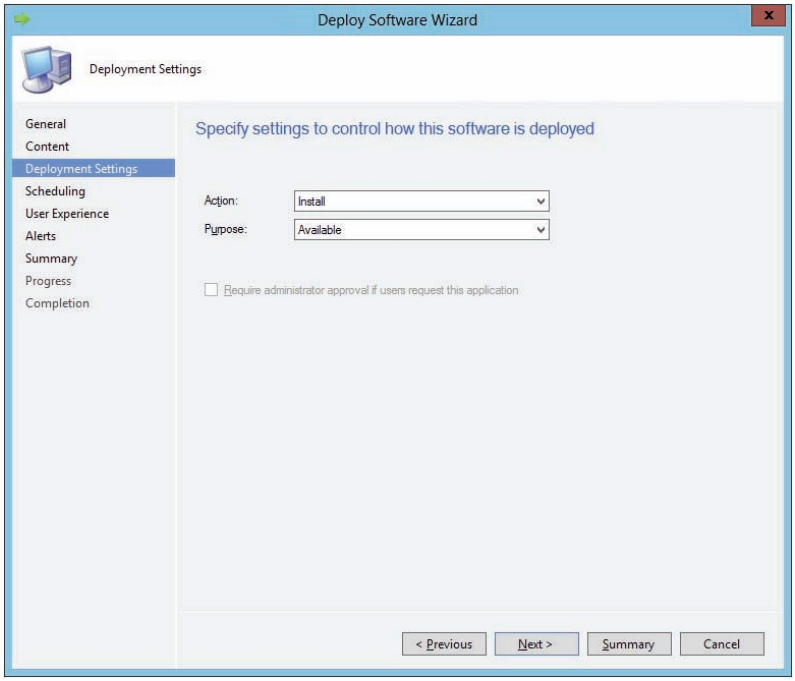


FIGURE 8.35
Deploy Software Wizard—Deployment Settings page

Action This setting is where administrators choose whether the deployment will act to install or uninstall the application.

Purpose This setting is where administrators choose whether the application simply is made available for manual installation, such as through the Software Center or the Web Catalog, or whether the application installation will be required.

If set to Required, the application will be enforced on targeted systems/users on the schedule specified. A change in Configuration Manager 2012—with the Required setting in place, the Configuration Manager 2012 client will periodically check to see if the application remains installed. If the application has been removed, it will be deployed again. As shown when discussing client settings earlier, the default detection cycle is weekly.

Require Administrator Approval If Users Request This Application If this application is targeted to a collection of users or user groups, this option becomes available and allows administrators to flag this application as one that will be listed as needing approval in the Application Catalog.

When you've finished with the settings on the Deployment Settings page, click Next to continue to the Scheduling page, shown in Figure 8.36.

The options available on the Scheduling page are dependent on the setting chosen for Purpose on the Deployment Settings page:

- When Purpose is set to Available, then the only scheduling option available will be one that allows administrators to schedule application availability.

- When Purpose is set to Required, then the administrator will additionally be able to schedule the deadline for installation, either as soon as possible or for a specific time.

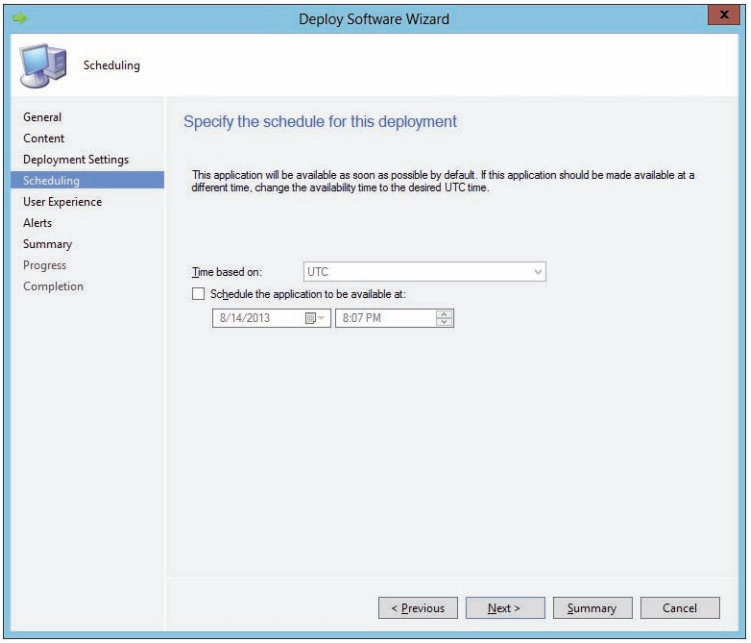


Figure 8.36
Deploy Software Wizard—Scheduling page

When you've finished with the settings on the Scheduling page, click Next to continue to the User Experience page, shown in Figure 8.37.

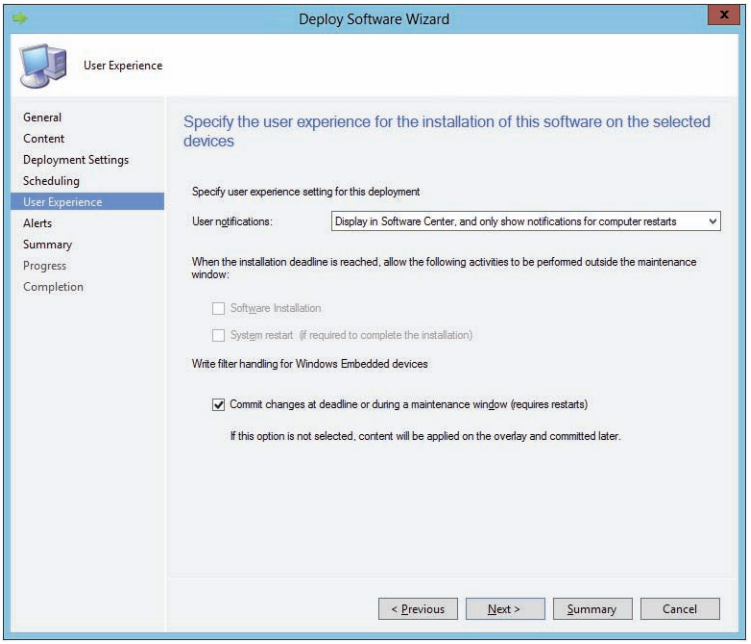


Figure 8.37
Deploy Software Wizard—User Experience page

The User Experience page allows administrators to configure user notifications. Available options are Display In Software Center And Show All Notifications or Display In Software Center, And Only Show Notifications For Computer Restarts. These options are self-explanatory.

The options for specifying activity to allow when an installation deadline has been reached are gray when the deployment is set with a Purpose of Available. When the deployment is set with a Purpose of Required, the options Software Installation and System Restart are configurable.

For Windows Embedded devices support is added for handling the write filters. You are able to commit the changes at the deadline or during a maintenance window, or the content will be applied in the overlay and committed in a later stage.

When you've finished with the settings on the User Experience page, click Next to continue to the Alerts page, shown in Figure 8.38.

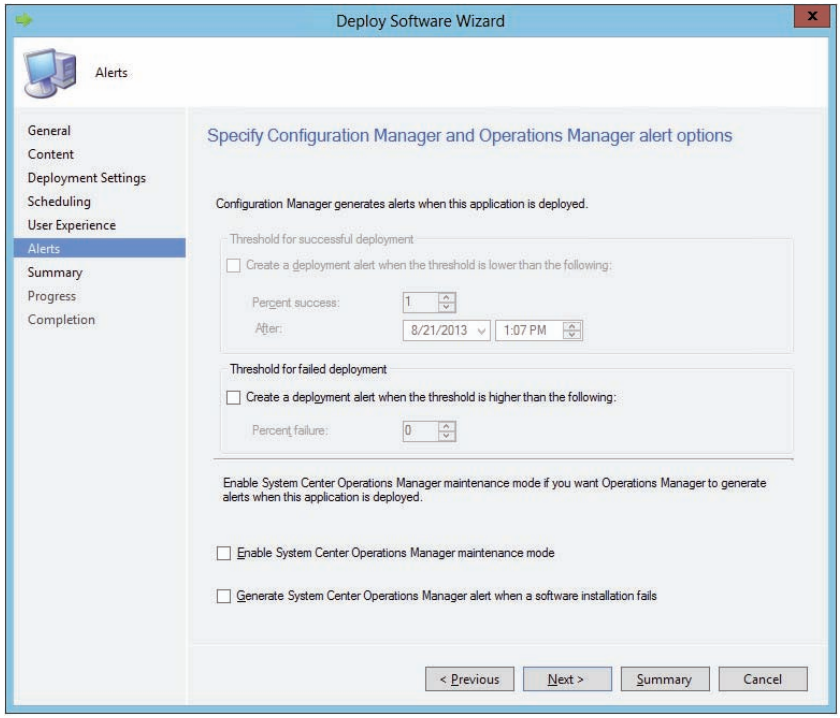


FIGURE 8.38 Deploy Software Wizard—Alerts page

The Alerts page allows administrators to configure criteria for when to generate alerts in response to deployment status. The alerting ability provided in Configuration Manager 2012 is new and provides an additional mechanism for awareness of deployment health.

Create A Deployment Alert When The Threshold Is Lower Than The Following This option allows administrators to specify a threshold of expected deployment success for a given deployment within a specific time frame. If the deployment success has not met or exceeded the configured threshold within the configured time, an alert will be generated to notify the administrator.

Create A Deployment Alert When The Threshold Is Higher Than The Following This option allows administrators to specify a threshold for a deployment that, if exceeded, will cause an alert to be triggered. This option would be useful in a scenario where a certain number of licenses have been purchased for an application. If a sufficient number of users install the application to cause the number of available licenses to near depletion, the administrator would be alerted and have the opportunity to either order additional licenses or scale back the usage of the application.

Enable System Center Operations Manager Maintenance Mode This option allows integration between Configuration Manager 2012 and Operations Manager. By selecting this option, when a deployment begins on a client, and if the client is also an Operations Manager agent, the agent will be placed in maintenance mode. After the deployment completes, the Operations Manager agent will be triggered to exit maintenance mode.

Generate System Center Operations Manager Alert When A Software Installation Fails This option causes an alert be generated in Operations Manager to raise immediate awareness when the installation of an application fails.

Monitoring deployments with System Center 2012 R2 Operations Manager

Although Operations Manager maintenance mode is beyond the scope of our discussion, one thing does need to be mentioned. This option does not cause true Operations Manager maintenance mode to start. Instead, the Health Service on the Operations Manager agent is simply paused for the duration of the application deployment. Once deployment completes, the health service resumes from that point in time without accounting for any problems that might have happened during application deployment, such as a system reboot. This is an effective approach to suppress noise in Operations Manager but will not be reflected as maintenance mode in the Operations Manager console.

Updated Integration Feature

In Configuration Manager 2007, this maintenance mode integration was not reliable. Configuration Manager 2012 has been updated so that this integration works as intended, regardless of platform.

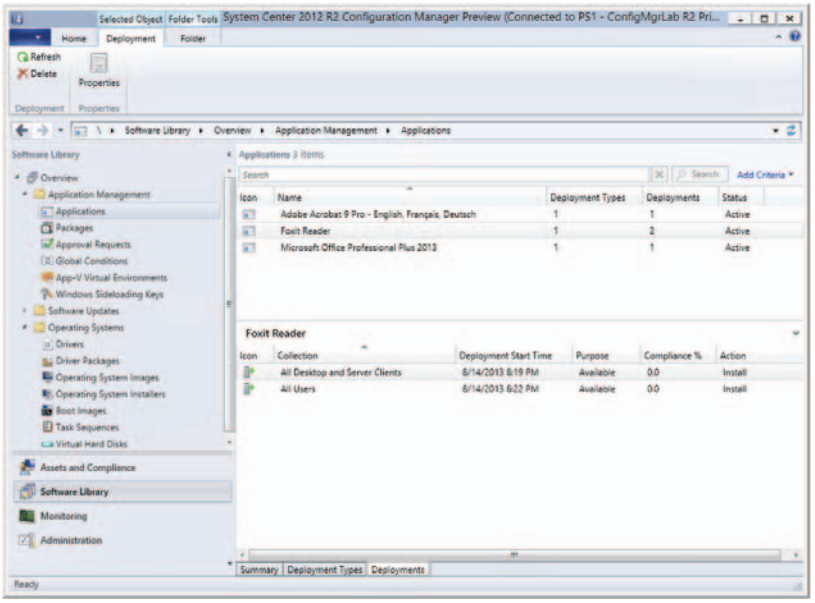
When you've finished with the settings on the Alerts page, click Next to continue to the Summary page. Review the settings on the Summary page. If they're all acceptable, click Next to save the configuration and then exit the wizard.

Application Deployment—Client Experience

The ultimate goal of Application Deployment is to take action on Configuration Manager 2012 clients. The work described so far has built an application deployment, a deployment type, and a deployment. The current sample was configured to be available and was targeted to a collection of devices. The current configurations will simply make the application available for install in the Software Center on all targeted clients.

As configured, the application will *not* show up in the user-centric Application Catalog. Inclusion in the Application Catalog requires that the application be deployed to a collection of users or user groups. To make the sample Foxit Reader application also show as available in the Application Catalog, a second deployment needs to be added. The only difference for this deployment is that a collection of users will be chosen rather than systems. The new deployment is shown in Figure 8.39.

FIGURE 8.39
Second deployment added, targeted to a user collection



With the second deployment added, the application now shows as available in both the Software Center and the Application Catalog. Take a look at the way the applications are presented in both and the descriptive information that is available. Looking at Figure 8.19 and Figure 8.20 you can see that the information you have supplied is presented in the Software Center in Figure 8.40 and the Application Catalog in Figure 8.41. It's good to understand how these configurations map between the different components so that when you configure an application, the user will have meaningful and descriptive information to review.

Client Application Installation

When an application is configured to be required, it will be installed regardless of whether the user requests it in the Software Center or selects it in the Application Catalog. In some cases, applications may be marked as required but also as visible in the Software Center and Application Catalog, but that is not automatic. For applications that should be optional for the user, simply mark them as being available and, depending on other configurations such as requirements, they will appear for the user in the Software Center. If the application is targeted to a user collection, it will also appear in the Application Catalog.

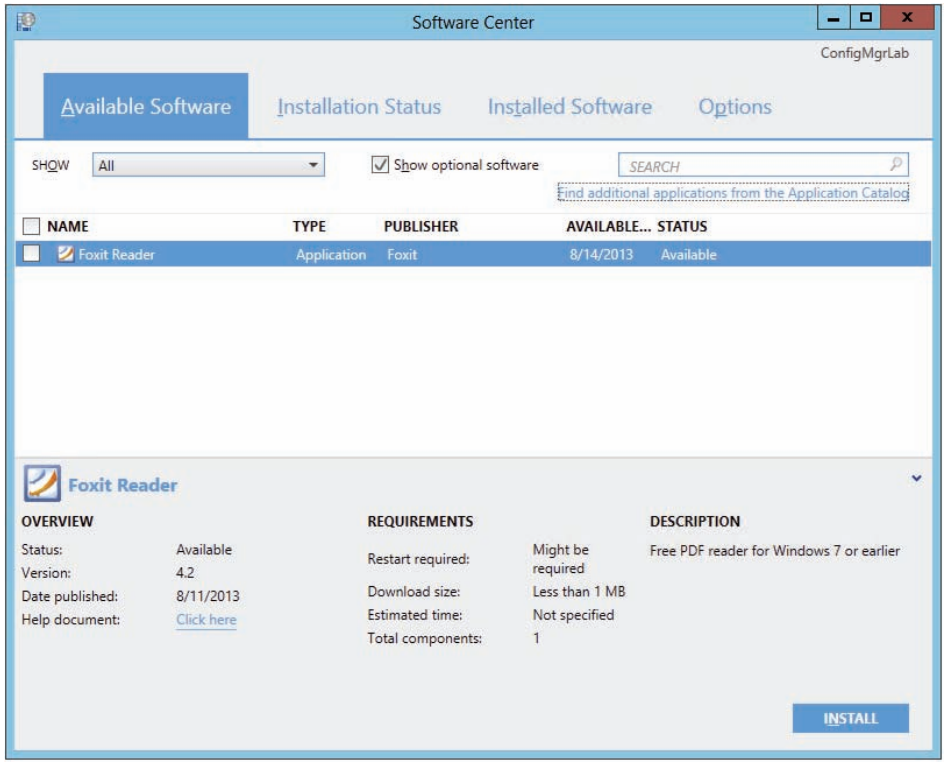


FIGURE 8.40
Foxit Reader 4.2 in the Software Center

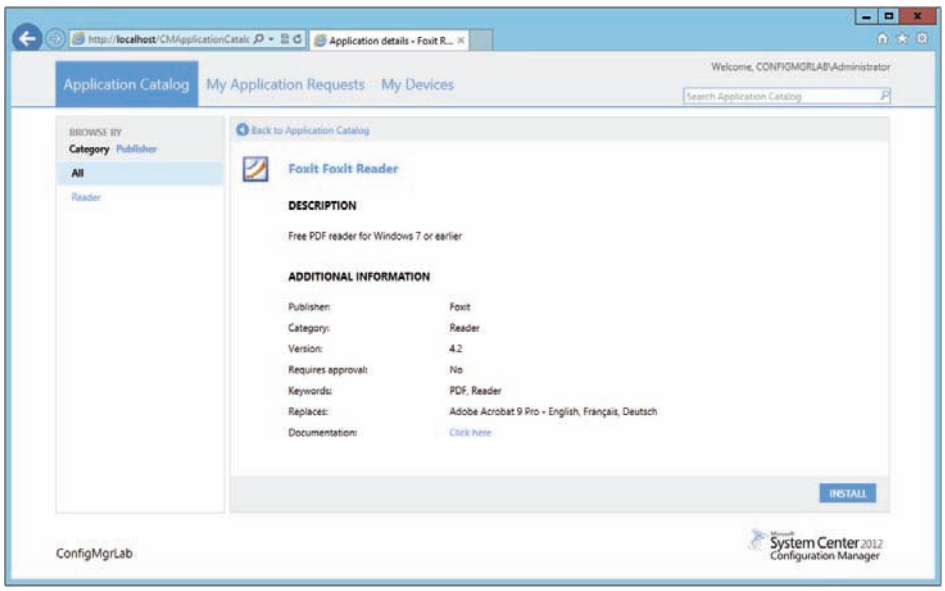


FIGURE 8.41
Foxit Reader 4.2 in the Application Catalog

Bottom line, the Software Center is available on each Configuration Manager 2012 client and allows the user to have control over at least some of their own experience with Configuration Manager 2012. As the name implies and as already discussed, the Software Center presents a list of applications to the user that are available for install, along with a good amount of potential detail to help the user understand the application. But the Software Center is more than just an application chooser. Click the Installed Software node, and you'll see that it is also useful for tracking software that has been installed on the system historically.

The Options node, also part of Software Center and shown in Figure 8.42, allows users to specify their own work information and maintenance settings. Think of these settings as a user-controlled maintenance window. By specifying business hours, users are configuring their system so that they are not disrupted by application installs or system reboots in the middle of the day. Maintenance settings work with Work Information settings to specify when the computer will be available for software installations. Ultimately, the Configuration Manager 2012 administrator retains full control even at this level because, when necessary, application deployment can be configured to proceed regardless of the settings specified.

Also available on the Options tab is the ability to configure local remote control settings and whether power management policy will apply to the system, but those topics are beyond the scope of software distribution, so we won't discuss them here.

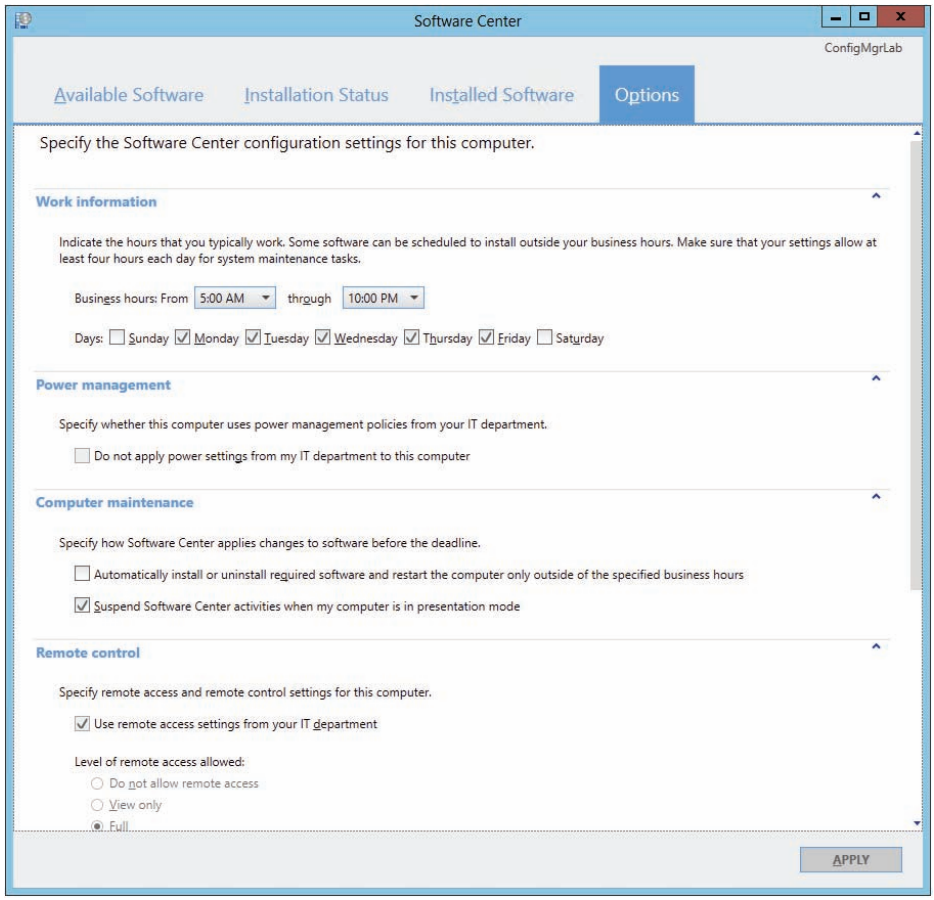


FIGURE 8.42
Software Center Options tab



Real World Scenario

Application Deployment—Beyond the Lab

Stepping through creation of the sample application is enough to start the wheels turning about ways this new model could be used in production. There is tremendous flexibility in the new Application Deployment model, but don't jump too far too fast. Spend time with the model and understand how things work before spinning up deployments in production. Remember, a lab environment is *much* more forgiving—and doesn't result in the need to explain problems to management!

In addition, there are many layers to the Application Deployment model. Explore each layer completely—from the rules-based Requirements engine to the ability to link applications together, known as references, creating a tie between applications that is useful for application upgrade. There is also the ability to verify that prerequisites are in place before deploying a given application. And don't forget a real gem of the new model, the ability to create multiple deployment types that can work with each other to detect information about the environment for the current deployment and deliver a version of the application best suited for each scenario; this includes deployments to devices, users, or both.

If you have trouble finding the right parameters for the setup of the application or the detection methods, a tool called Setup Commander can help you to create the deployment type with the right parameters and detection methods for lots of common software based on MSI setups and older legacy setups. Look for more information at `www.setupcommander.com`.

Application Deployment—Advanced Configurations

The steps just discussed demonstrated how to configure a basic application, deployment type, and deployment. These building blocks are pivotal to understanding the Configuration Manager 2012 Application Deployment model but in some ways just scratch the surface of what is possible. We've already mentioned several additional and more complex configurations but have not discussed them in any detail. This section takes a step back and reviews these additional configurations. With Application Deployment, all of the various configurations and options that are possible are simply too numerous to cover individually, but the hope is that with the discussion provided you will be able to see the possibilities, flexibility, and power available.

Supersedence

This example builds on the previous one by adding an additional deployment that is configured to deploy Adobe Acrobat 9 Pro. In this example the Configuration Manager admin must cut costs and replace the paid version of Adobe Acrobat 9 Pro with Foxit Reader, which is free. This introduces the first point of discussion: *supersedence*. In the definition of the application it is possible to configure a relationship where one application supersedes another application. This type of relationship is extremely valuable to maintain control of the application upgrade process and also to define how one application should operate during the upgrade process—but that's jumping a bit too far ahead.

Configuring a supersedence relationship is easy. Simply do the following:

1. Open the properties of the application where a supersedence relationship is to be defined.
2. Click Browse.
3. Select the application that the current one should supersede, and then click OK.

The result is shown in Figure 8.43.

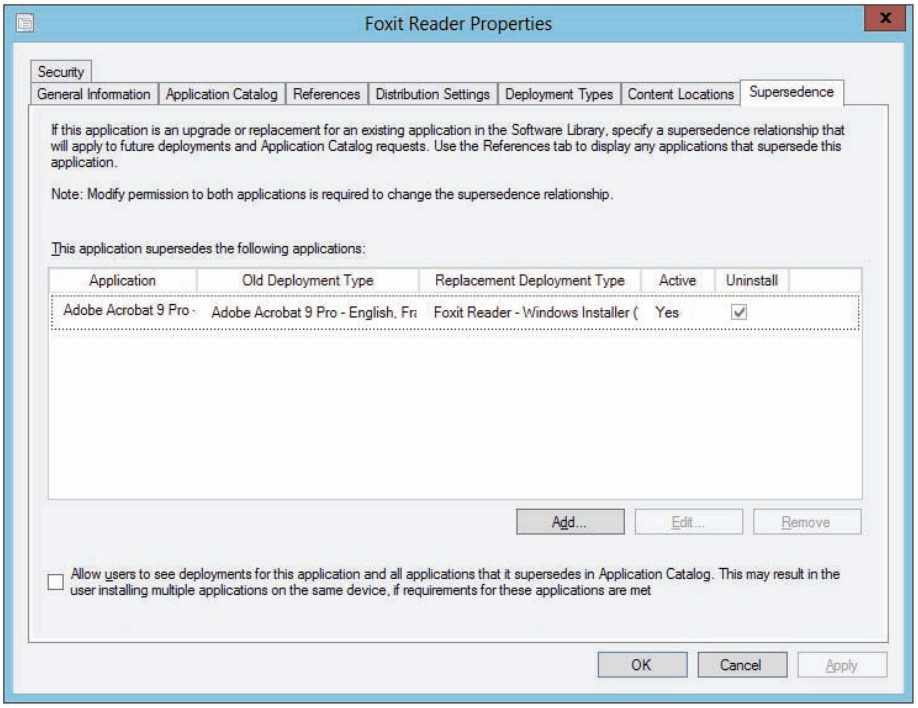
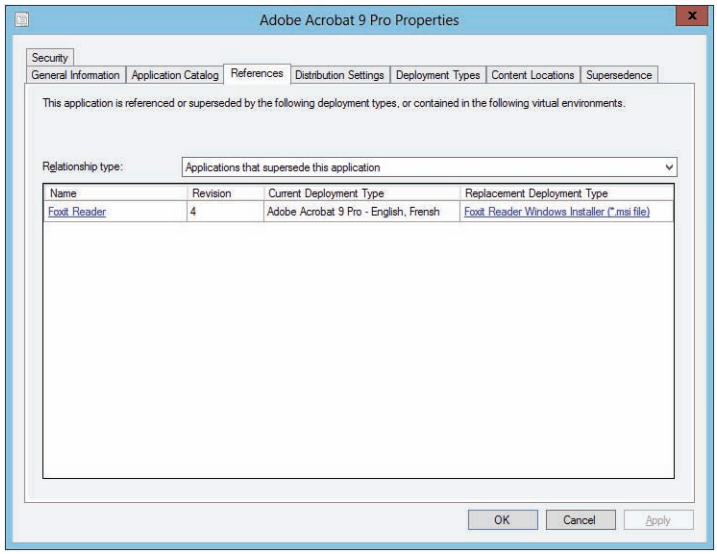


FIGURE 8.43 Supersedence relationship added to Foxit Reader application

Notice that when defining a supersedence relationship it is possible to specify whether the application being replaced should first be uninstalled. When selecting to uninstall an application, make sure that the uninstall command line setting for the previous application has been configured properly to accommodate the uninstall. A further configuration allows specifying which deployment type from the current application will be used during deployment.

To see the results of creating the supersedence relationship, simply look at the properties for the Adobe Acrobat 9 Pro application and select the References tab. There are three options for viewing data on this tab: Applications That Depend On This Application, Applications That Supersede This Application, and Virtual Environments That Contain This Application. For the current purpose, select the second option, which will show that the Foxit Reader application now supersedes the Adobe Acrobat 9 Pro application. This is shown in Figure 8.44.

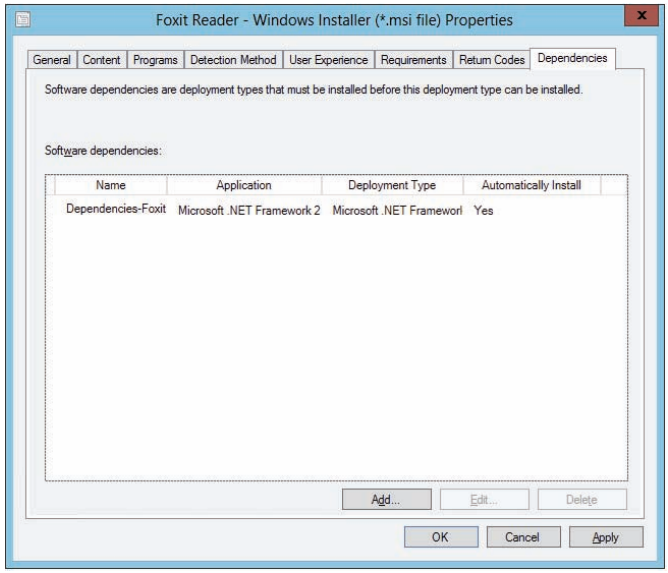
Figure 8.44
Supersedence reference



Dependencies

Going back to the deployment type for the sample Foxit Reader application, it's time to configure a dependency. The dependency option specifically allows administrators to define software that must be installed before the current application can be deployed. The dependency option is not a vehicle to specify any other kind of requirement. As shown in Figure 8.45, the sample Foxit Reader application is configured to require that .NET Framework 2.0 be installed first. If this requirement isn't met, and depending on the setting for the Automatically Install option, either the application installation will fail or the application installation will pause while .NET Framework installation completes.

Figure 8.45
Dependency configuration



Detection Method

The ability to detect whether a dependency is installed or not depends on whether settings to do so are specified in the Detection Method tab for an application. Dependencies also allow administrators to configure potentially complex dependency relationships to ensure all needed applications are present before proceeding with a deployment.

Detections methods are also useful to determine whether a given application has already been deployed to a target system. If so, there is no need to deploy it again, and the application deployment will simply exit.

If a user, for instance, removed the application from the computer and the Application Deployment evaluation cycle detects that an application is not installed, the application will be installed (again).

You can create detection configurations to check the filesystem, a registry location or value, an MSI GUID, or a combination of these settings to determine if a given application is present. When you use the wizard to build an application deployment based on an MSI, as in the Foxit Reader example, the detection information is supplied by default. Figure 8.28, shown earlier, is a view of the Detection Method tab.

Besides the standard detection methods, custom PowerShell, JScript, or VBScript scripts can also be used to detect if an application is installed or not.

Requirements

When deploying an application, administrators may wish to specify rules to govern the application install. The Requirements tab of the deployment type allows deployment rules to be configured, from simple to complex. You can build rules to check attributes related to the device or user being targeted or build custom rules to cover most any scenario. The conditions that are available for both device and user-targeted applications are shown in Table 8.3.

Table 8.3: Rule options

Device	User
Active Directory site	Primary device*
Configuration Manager site	
CPU speed	
Disk space	
Number of processors	
Operating system	
Operating system language	

Device	User
Organizational unit (OU)	
Ownership	
Total physical memory	
Windows Store inactive	

**The primary device and its use for application deployment will be discussed along with user affinity.*

The mechanisms available for building custom rules are as follows:

Active Directory query

Assembly

Filesystem

IIS Metabase

Registry key

Registry value

Script

SQL query

WQL query

XPath query

As is noted by the combination of the rule options shown, literally any possible scenario can be covered by specifying the right type of rule.

For the sample Foxit Reader application, the only systems that should install it are those that run Windows 2008 or better and already have the superseded application, Adobe Acrobat 9 Pro, installed. Figure 8.46 shows the completed Requirements node, which details the checks that must pass before proceeding with application deployment.

It's interesting to note regarding the Requirements tab that when Configuration Manager 2012 clients receive notification of a new application and if that application has a list of requirements, those requirements will be evaluated upon receipt of the deployment policy, and if the requirements for deployment are not met, the application will not be displayed as available for deployment on the target system. Applications are evaluated periodically to determine if the conditions specified by the requirements have changed.

The rules available for use in the Requirements tab are visible in the Software Library ➢ Overview ➢ Application Management ➢ Global Conditions node of the console. The list will also include any custom requirements that may be created. This is shown in Figure 8.47. Note that the custom global condition just created is stored in the list and selected.

Global conditions can also be created from the node shown in Figure 8.47, when selecting the Create Global Condition option in the Home tab of the ribbon in the Configuration Manager 2012 console. The custom-created global conditions can be used in other applications throughout the hierarchy.

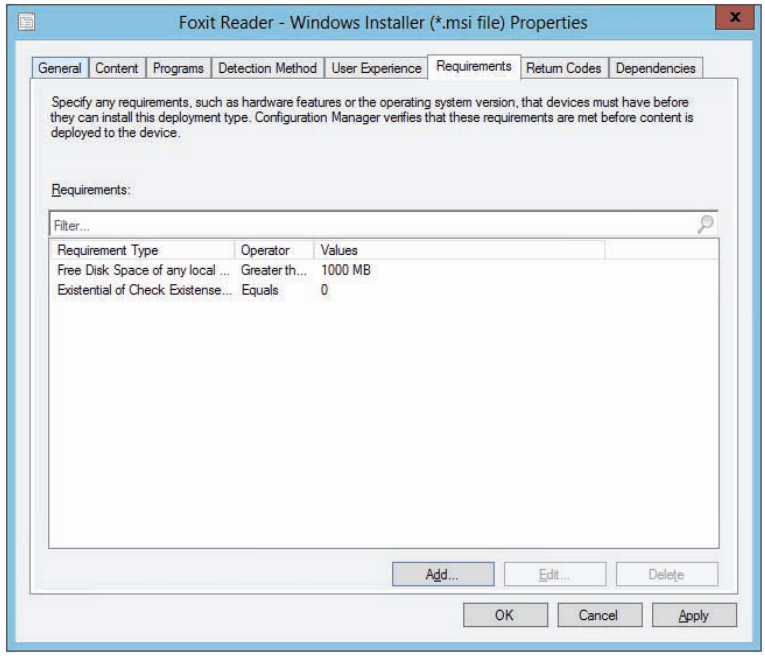


FIGURE 8.46
Requirements node completed

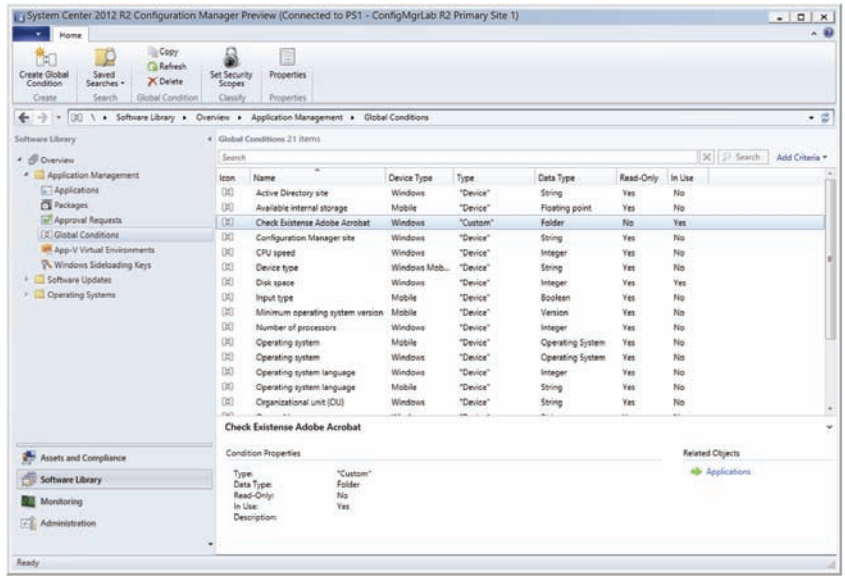


FIGURE 8.47
Global Conditions node

When retrieving the properties of the custom-created global condition, you can review the references and see in what application the global condition is used, as shown in Figure 8.48.

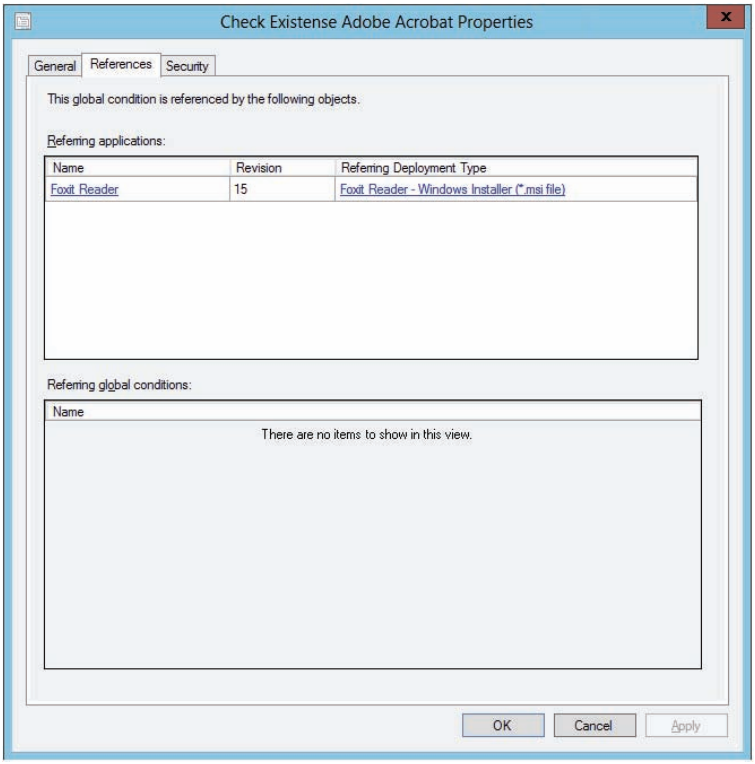


Figure 8.48
Reviewing the references of the Custom Global Condition

Deploying Applications Other Than MSI and Scripts

Not only MSI files, executables, or scripts can be deployed to users or devices. Configuration Manager 2012 R2 has more deployment types available. Since Chapter 16 is all about mobile device management, we focus here on the applications that can be deployed to Windows, Unix/Linux, or Mac OS X–based devices.

Application Virtualization 4.6/5

When you have sequenced an App-V 4.6 or App-V 5 application, you can deploy this application to devices depending on the requirement rules. Both App-V clients need to be deployed separately and are not included with Configuration Manager 2012.

In Configuration Manager 2012 you can create virtual environments for App-V 5. App-V applications in a virtual environment share the same filesystem and registry; this way the applications can interact with each other. You can create App-V virtual environments in the Software Library ➢ Overview ➢ Application Management ➢ App-V Virtual Environments node of the console, as shown in Figure 8.49.

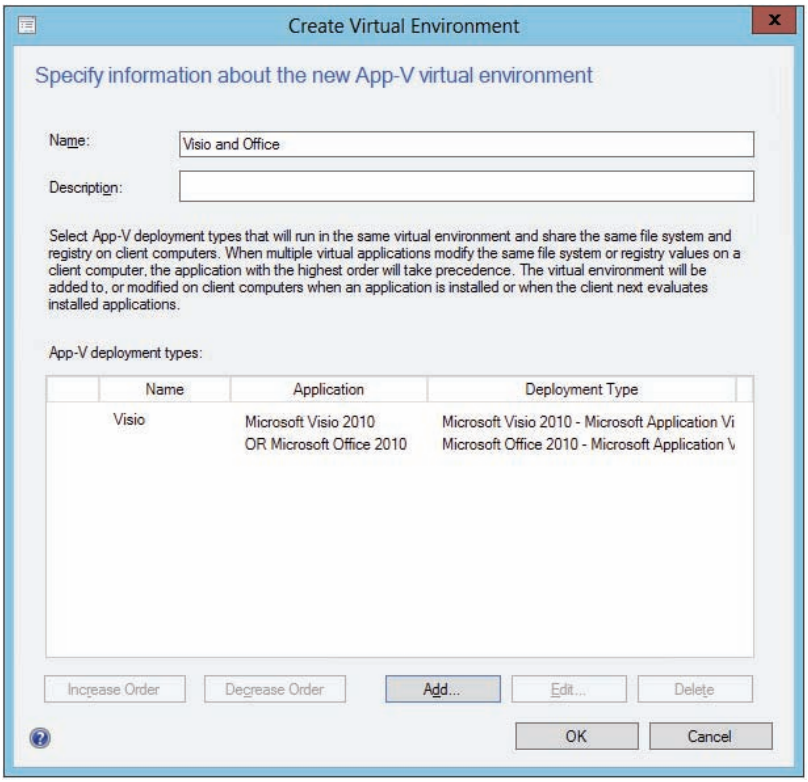


FIGURE 8.49
App-V virtual environment for Office 2010 and Visio 2010

Windows 8 Modern Applications

Deploying Windows 8 Modern applications for Windows 8.1 or Windows RT devices can be done in two different ways:

- Installing the application from the online Windows Store
- Installing the application from the distribution point, called sideloading the application

When you want to install an application from the online Windows Store, you need to install the application first on a Windows 8 reference computer. When selecting the Windows app in the Windows Store deployment type, you need to click Browse to be able to connect to the reference computer. Once you are connected, you should see a list like the one shown in Figure 8.50. Select the application you want and deploy it to your clients.

When you select the application from the Software Catalog you want to install, it will redirect you to the application in the Windows Store. You can install the application from the Windows Store.

To be able to sideload a Windows 8 line-of-business application, you need a trusted certificate to sign the application, since it is not signed by the Windows Store. This can be a trusted certificate from your own certificate authority or one from the trusted root CA such as VeriSign, GlobalSign, or Symantec. Using an external trusted root is a best practice.

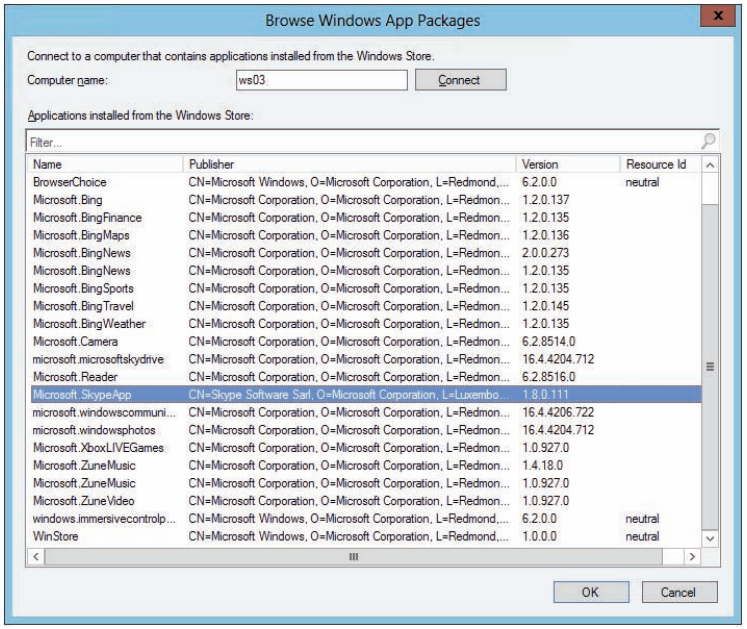


Figure 8.50
Select an application that is installed on the reference computer.

You also need sideloading product activation keys for every device you want to sideload an application to. These keys can be acquired at the Microsoft Volume License website. Once you have the sideloading product activation keys, you need to add them to Configuration Manager. You can add these keys in the Software Library ➢ Overview ➢ Application Management ➢ Windows Sideloading Keys node of the console. Click Create Sideloading Key to enable sideloading of applications for Windows RT, Windows RT 8.1, and Windows 8.1. This opens the Specify Sideloading Key dialog shown in Figure 8.51.



Figure 8.51
Adding sideloading keys

If you want to create and deploy a custom-developed application, you need to acquire a Microsoft developer license. Once you have the license, you can create a custom application, sign it, and sideload it via Configuration Manager.

Mac OS X

Configuration Manager 2012 supports the deployment of Mac OS X applications to the supported Mac OS X versions described in Chapter 2. Deploying an application to a Mac is somewhat different than deploying it to a Windows device using the new application model. Deploying the Mac OS X application is done with the new Mac OS X deployment type but has the following limitations:

- You need to first convert the Mac application package to a format that Configuration Manager 2012 recognizes and supports. You can convert the Mac application package with the `CMAppUtil` tool that comes with the Configuration Manager client for the Mac OS X platform.
- Applications cannot be deployed to users but only to devices. Predeploying software to the user's primary device is not supported.
- Mac applications support simulated deployments, allowing you to test your requirement rules.
- Global conditions are not supported when you create deployment types for Mac OS X computers.
- All deployments must have a purpose of Required. There is no Software Center available for the Mac OS X.
- BITS is not supported on Mac computers. When a download of the content fails, the entire download will restart.
- Wake On LAN via the deployment is not supported on Mac computers.

The first step if you want to deploy an application to a Mac OS X computer is to convert the application to the Configuration Manager 2012–supported CMMAC format. The following application packages can be converted:

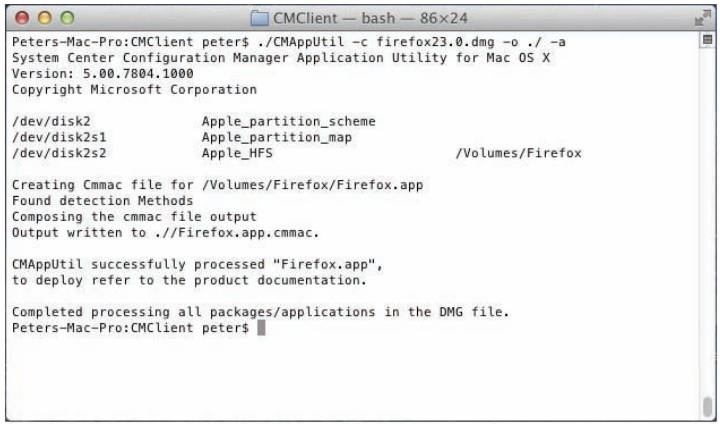
- Apple Disk Image (`.dmg`)
- Meta Package File (`.mpkg`)
- Mac OS X Installer Package (`.pkg`)
- Mac OS X Application (`.app`)

For example, we want to deploy Firefox, which comes in `.dmg` format (`Firefox 23.dmg`). The Configuration Manager 2012 client for the Mac includes the tool `CMAppUtil`. This tool can be found in the `Tools` folder after extracting the compressed file.

Running the following command will result in a `Firefox23.0.cmmac` file, as shown in Figure 8.52.

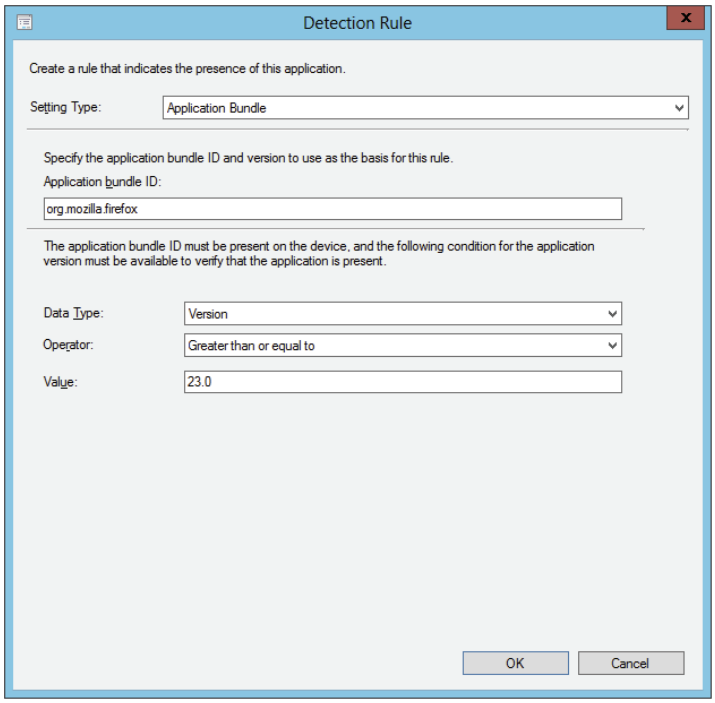
```
./CMAppUtil -c firefox23.0.dmg -o ./ -a
```

FIGURE 8.52
The DMG file is converted to a CMMAC file.



After you import the CMMAC file for Firefox, all the necessary information including the detection method is automatically configured. Figure 8.53 shows the detection method configured for detecting the application bundle org.mozilla.firefox version 23.0.

FIGURE 8.53
Detection method for a Mac OS X application



As mentioned, the application needs to be deployed to the Mac OS X device; it will be installed when the Configuration Manager 2012 client connects to the primary site.

Linux and Unix Applications

When you need to deploy an application to a Linux or Unix server, you will need the classic packages and programs instead of an application. With the classic packages you can deploy new software, operating system patches, and software updates for programs that are already installed on the server.

When deploying a Linux or Unix application to a server, you need to keep the following in mind:

- You should learn how to use and manage Linux or Unix, or you can ask the administrator of those servers to deliver the scripts that can be used to deploy the software or updates.
- You can run only native Linux and Unix commands.
- You can run only scripts that are already located on the Linux or Unix server.
- You can create a program for specific operating systems by selecting the option This Program Can Run Only On Specified Platforms, as shown in Figure 8.54.

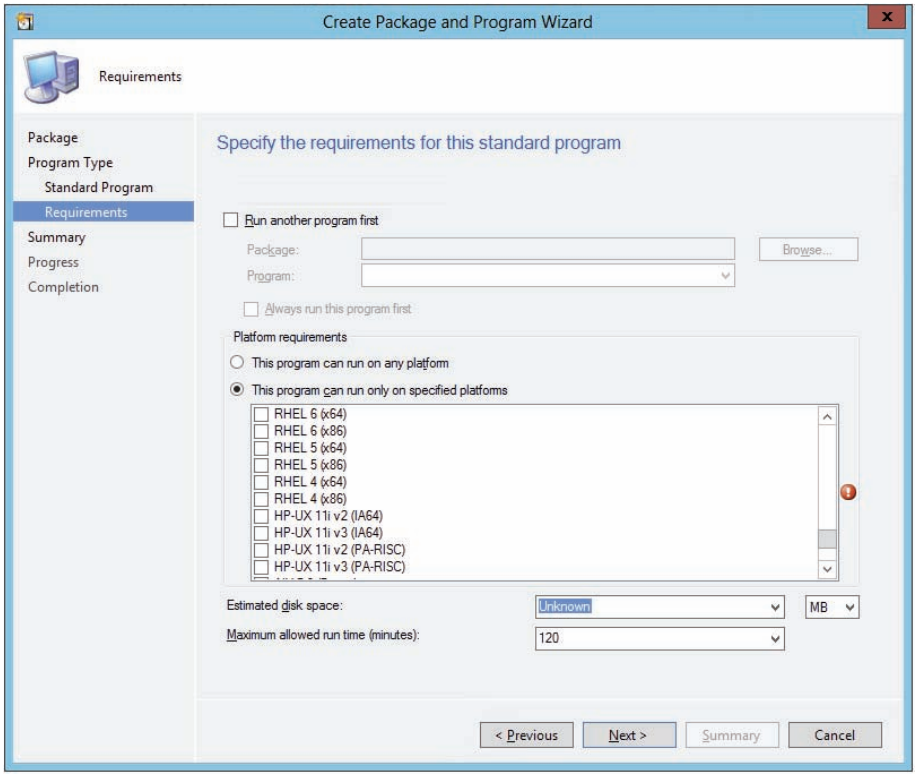


FIGURE 8.54 Select the platform for which the program is created.

- The Configuration Manager client for Linux and Unix does not support the deployment of scripts that make user environment configuration changes.
- The Network Access account is used to download the content from the distribution points.
- Only deployments with a Required purpose are supported.
- Include file types in the scripts that are supported on the destination operating systems.

Web Application

A web application is a link to a website; this deployment type installs a link on the device of the user.

User Device Affinity

As already described, the Application Deployment model in Configuration Manager 2012 is extremely flexible and provides administrators many options for delivering content. Configuration Manager 2012 provides flexibility in delivering applications to users so that users, regardless of what device they are using, will have a consistent experience. As an example, if a user is logged onto their primary device, then an application may be configured to be installed on the target system, whereas if a user is simply logged onto a shared computer, they may instead receive a virtualized copy of the application. If the user is logged onto a mobile device and a mobile version of an application is available, further options to accommodate software deployment are available there as well. Whatever the case, the user's experience is that their required software is available, but the administrator has control over how the software is provided.

In order for a user to be properly detected as logged onto their primary device rather than a shared device, a mechanism must be in place to guide that decision. User Device Affinity settings provide that mechanism.

User Device Affinity allows a user to be associated with their primary device(s). User Device Affinity associations are configured in one of several ways:

- The user can configure that a device should be considered a primary device in the Application Catalog.
- The administrator can configure the My Devices option in the Application Catalog, shown in Figure 8.55.
- You can use a file to map a user to their primary device(s) and then import this file to Configuration Manager 2012.
- You can choose the option Import User Device Affinity settings, which is available in the Assets and Compliance node of the console. The Import User Device Affinity Wizard is shown in Figure 8.56.

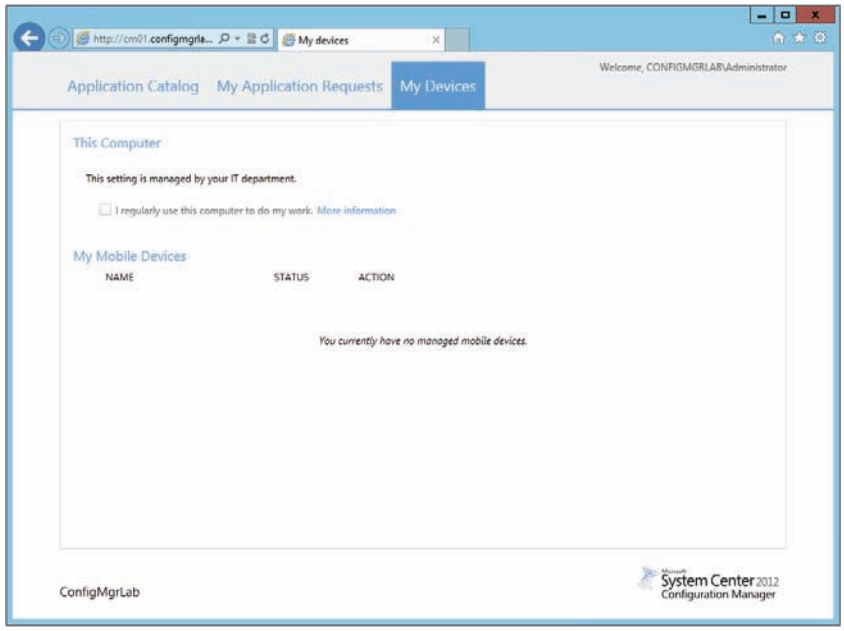


FIGURE 8.55
User-configurable Device Affinity option

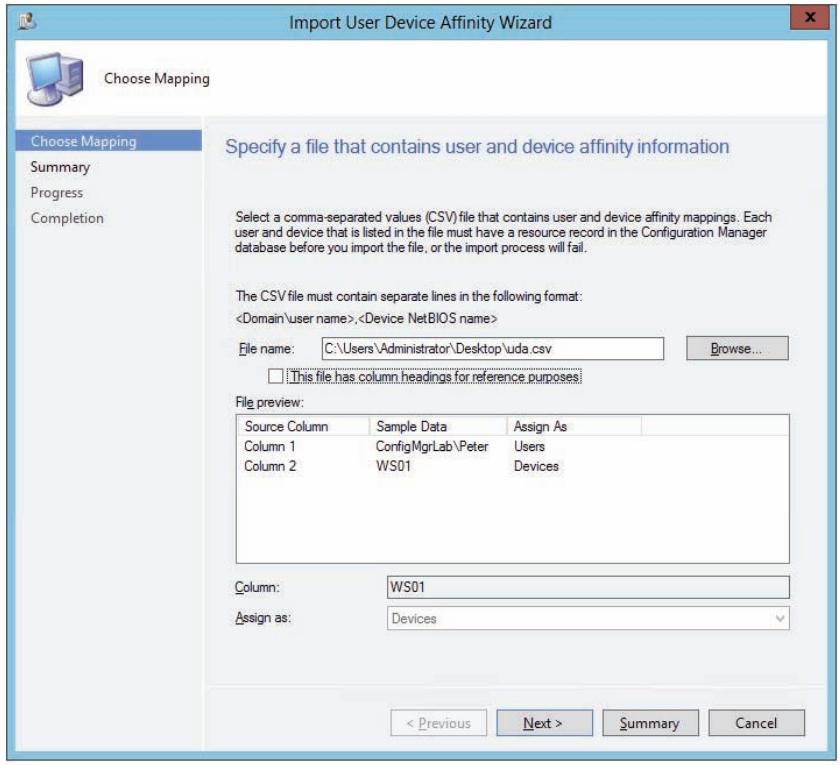


FIGURE 8.56
Import User Device Affinity Wizard screen

- You can configure Configuration Manager 2012 to automatically build user-to-primary device mappings based on information collected about devices used by a user. With this method administrators retain control over whether to automatically accept the detected settings.
- Configuration Manager 2012 can be configured to automatically detect primary device mappings through usage data, as shown in Figure 8.57. The default setting does not allow to automatically configure the user device affinity. Note that the required inventory class in the Hardware Inventory, SMS_SystemConsoleUsage, is enabled by default.

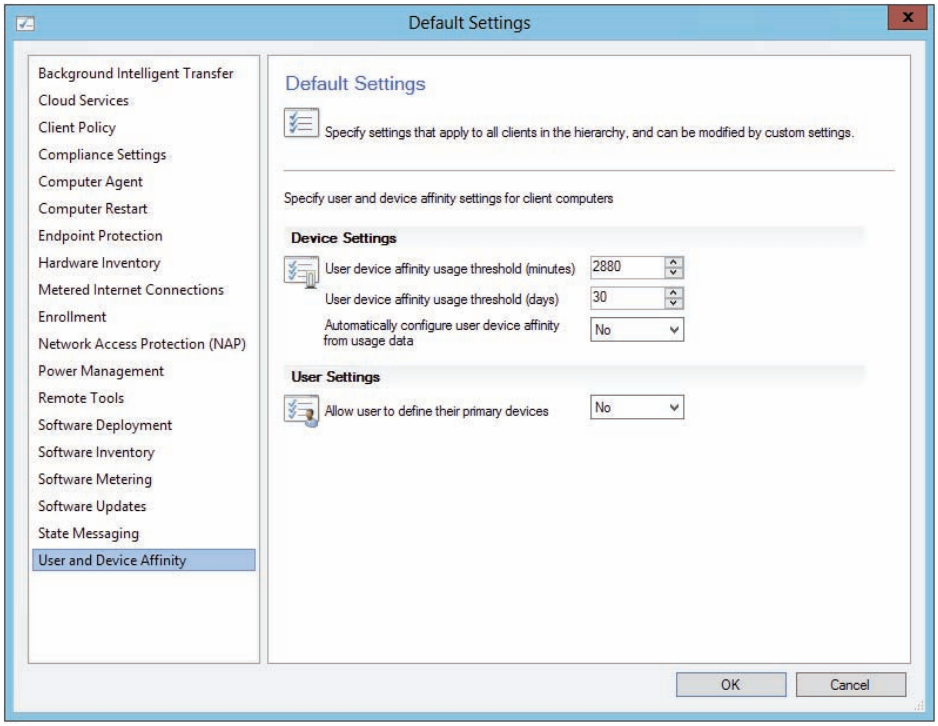


Figure 8.57 Configuring automatic user device affinity detection

- The Configuration Manager 2012 administrator can manually create relationships between users and device(s) by using the Edit Primary Devices node in the console. This is shown in Figure 8.58.

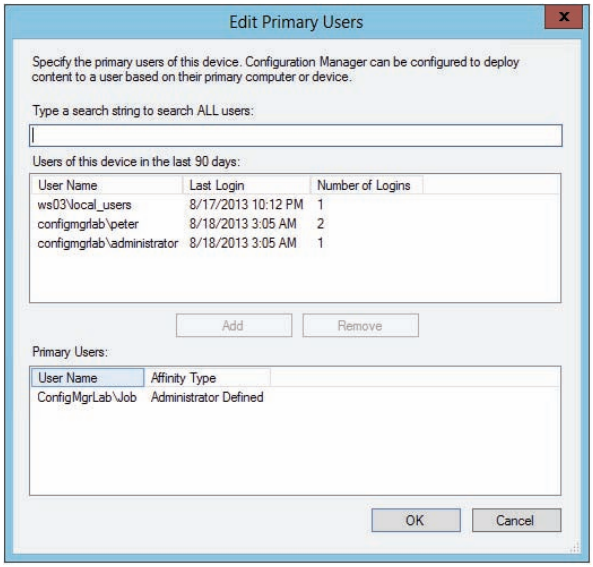


FIGURE 8.58
Edit Primary Users

- Specific to mobile devices, when a user enrolls a device, a relationship is automatically created between the user and the mobile device.

Also note that the User and Device Affinity settings are not limited to specifying one primary device per user. Very often a single user may have more than one primary device, such as a computer, as well as a mobile device. It's also possible that a given device will be the primary device for multiple users, such as in a shared workstation scenario. Configuration Manager 2012 handles any of these device-to-user mapping scenarios.

Troubleshooting Application Deployment

With any product, in-depth troubleshooting requires a good understanding of the overall system to know where to look and common things that might go wrong. Configuration Manager 2012 is a large product with many moving parts, so understanding how to troubleshoot effectively comes with experience. The depth of troubleshooting attempted will depend on available time and your experience level with the system. The latter will grow over time. Chapter 19, "Troubleshooting," discusses the troubleshooting options for Configuration Manager 2012 in general. It is useful to spend a few paragraphs discussing troubleshooting as it relates to Application Deployment. The intention here will be to augment the troubleshooting discussion from Chapter 19.

Monitoring

Configuration Manager 2012 is built to help administrators stay updated on the progress of various work and to flag when a problem is encountered; the Monitoring section of the console is designed specifically with that purpose in mind. Figure 8.59 shows the Deployments node of the Monitoring section.

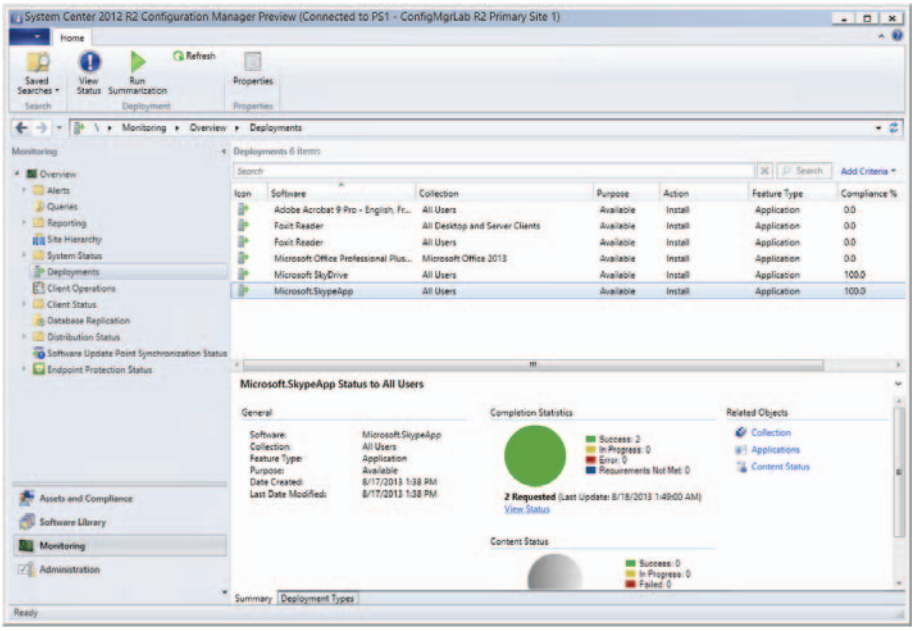


FIGURE 8.59
Deployments node of the Monitoring section

The Deployments node allows administrators to see at a glance the progress of deployments in the environment. The top section of the screen is just a summary. Note that the sample Foxit Reader deployment is listed twice, one instance being the deployment targeted to users and the other instance targeted to systems. In this node it might be possible that a given deployment is shown as 100 percent compliant, yet no systems may have attempted to run the Foxit Reader application yet. Why might that be the case? In this case, compliance reflects that 100 percent of the targeted systems have accepted the deployment and reported back with a status.

This would mean that the systems reporting back have evaluated the deployment and found it to fail the deployment validation—so status is reported back but no install is attempted. Taking this type of logic further, consider if this application had been delivered to a collection with six systems, but we receive status back for only two. Does that mean the other four are having issues? Maybe but not necessarily. If the application requirements exclude deployment to the other four systems, then they won't even show up. Remember what was mentioned earlier about how it is feasible to deploy everything to the All Systems collection provided sufficient requirements are in place for an application? This is an example of how that would work. To restate, deploying to the All Systems collection is not recommended, but it would be possible.

From the Summary view it is also possible to review the target collection, the state of the software, and the status of deployed content (see Figure 8.60).

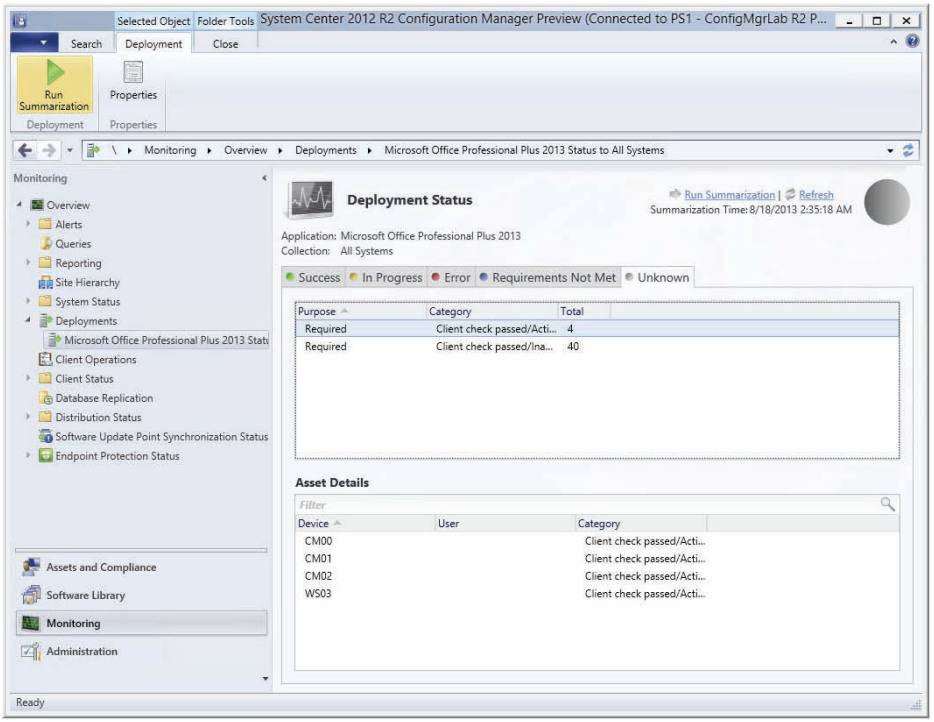


Figure 8.60
Deployment status

Deployment Status

The information available here is critical for understanding the actual state of a deployment. If a deployment has been configured but is not showing up on targeted systems, your initial thought might be that something isn't working right. That may be, but more likely the problem is not with the system but with some configuration. In this case, the deployment arrived at the client, failed requirement evaluation, and simply wasn't made available. The pie chart (Figure 8.60) and detail data lead right to the problem. Without them, an administrator would need to look elsewhere for the source of the problem.

Log Files

Configuration Manager 2012 provides an extensive set of log files to aid administrators in troubleshooting scenarios. The information provided by the log files is significant, but even more detail is possible if you configure verbose or debug logging (covered in Chapter 19).

Logs in Configuration Manager 2012 are very beneficial for experienced administrators to quickly pinpoint a problem. For beginning administrators, though, the logs may be

intimidating. Experience will help increase your comfort level with logs. A few suggestions will help keep things on track:

- Determine which logs to review.

  Configuration Manager 2012 processes generally can be broken into processing that happens on the server and processing that happens on the client. The management point is in the middle and can have elements that interact with both the server and the client. The place to start reviewing log information depends on where the processing problem seems to be happening: server side or client side.

- Be patient.

  The logging system in Configuration Manager 2012 is extensive, and finding the right log to review at first might be challenging. Many different Configuration Manager 2012 client components are required when trying to process an application deployment. These components pass information back and forth as the work gets done. With experience it becomes easier to know which log to start with, and it's well worth learning. Never fear though; if it gets too time consuming to dig through the information provided, Microsoft support is just a phone call away.

- Watch the time stamp.

  Following data in the log files boils down to following the time stamps. As logs update, their time stamps do too. A quick look at which logs have been active recently will help you identify logs that might be good candidates for review after an action is attempted and a failure encountered.

- Use CMTrace.

  The log files are viewable with Notepad, but it's definitely not the best environment. The CMTrace utility (formerly known as Trace32) available in Configuration Manager is perfect for viewing Configuration Manager logs—and many other types of text logs as well. Trace includes an error-lookup capability, the ability to filter by keyword or processing thread, the ability to merge log files to view the entire conversation between components (remember the time stamp discussion?), and so on. The utility has been updated for Configuration Manager 2012.

The Bottom Line

Explain the options available for Application Deployment. The new Application Deployment model is a significant and welcome change for deploying software in the enterprise. There are many new components including a rules-based Requirements engine, the ability to detect whether the application is already installed, the option to configure application dependencies and relationships, and more.

Master It List several configuration options available for applications and deployment types.

Detail the various components required for Application Deployment. Success with Application Deployment requires that several other Configuration Manager 2012 components be available and properly configured. The list includes management point(s), distribution point(s), IIS, BITS, the client itself, and possibly more.

Master It List the components required for configuring an application deployment.

Understand the role of and manage distribution points. The role of distribution points has not changed significantly in that this is the role that makes content available to Configuration Manager 2012 devices and users. The options available for implementing the role have changed significantly with the inclusion of throttling control content flow from site server to remote distribution points, the single-instance storage approach for placing content on distribution points, the ability to detect content corruption, and the requirement that all distribution points be BITS enabled.

Master It Discuss the differences between implementing a distribution point role on the site server locally and remotely.



Chapter 9

Software Updates

Ever since the I Love You (ILoveyou) worm hit the Internet in May 2000 and the Nimda worm hit the Internet in September 2001, patch management has become a very important part of maintaining network security. Those worms revealed the importance of patch management because it was vulnerabilities in Windows that had allowed the worm to spread so fast around the world, and Microsoft had released patches for these vulnerabilities several months earlier.

At the time, patching an operating system was a very labor-intensive task. Windows Update was available, but you still had to run it manually on each machine that needed updates. This meant connecting to the Internet, which was really too dangerous for corporate networks while ILoveyou and Nimda were spreading. As a result, network administrators and PC support staff ended up traveling to all their computers with a CD full of updates to get them patched up and safe again.

Microsoft released Software Update Services in 2002, and System Management Server (SMS) 2.0 got some patch-management functionality through an add-on feature pack. However, it wasn't really until SMS 2003 that there was a truly functional patch-management solution for the corporate enterprise. SMS 2003 used Microsoft Update technology to detect and install its updates, and it allowed reporting to show the progress. This was not without its problems; as more and more patches became available for Microsoft's operating systems and applications, this patch solution became more taxing on server and workstation resources.

The Software Updates feature in Configuration Manager 2007 was rewritten from the ground up and made the software update process even more effective by leveraging the Windows Server Update Services (WSUS) product and incorporating its capabilities into patch management and also by taking some of the load off Configuration Manager clients in the process. With the introduction of Configuration Manager 2012, Microsoft made configuring, deploying, and maintaining the software update role much easier than before.

In this chapter, you will learn to

- Plan to use Software Updates
- Configure Software Updates
- Use the Software Updates feature to manage software updates
- Use automatic update deployment to deploy software updates

What's New in Software Updates

After integrating Windows Server Update Services in Configuration Manager 2007 as the Software Updates feature, Microsoft further enhanced the feature in Configuration Manager 2012. With Configuration Manager 2012 you can manage your software updates more easily and quickly. The following changes and enhancements are available in Configuration Manager 2012:

Software Update Groups New in Configuration Manager 2012 are the software update groups; these replace the update lists that were available in Configuration Manager 2007. When you want to organize your software updates in your environment effectively, you need to use software update groups. With automatic deployment rules you can add new updates automatically, or you can add them yourself manually. The deployment of software update groups can also be done automatically or manually.

With software update groups you are also able to retrieve compliance information from devices for the software updates without deploying them.

Automatic Deployment Rules Software update administrators will have a ball with this new feature. With automatic deployment rules you can automatically approve and deploy software updates. You can specify criteria for software updates, and the software updates are automatically added to the software update group. When creating an automatic deployment rule, you can, for instance, use all Windows 8 updates released since the last Patch Tuesday; this way the Windows 8 updates will be automatically added to the software update group. When a deployment for the software update group is available, the software updates will be automatically rolled out to your clients.

Software Update Filtering The new Configuration Manager 2012 console has a good search engine; this search engine is also used for searching or filtering software updates. While defining a search, you can add a set of criteria that makes it easy to filter and find the updates you need. You can save the defined criteria when you are finished and use the criteria at a later stage.

With the results of the search you can select those software updates and add them to an existing or new software update group. You can also see the compliance information about the selected updates.

Software Update Monitoring The in-console monitoring feature is also implemented in the Software Updates feature. The Configuration Manager 2012 console provides real-time monitoring information about software updates and running processes. For instance, you can view the following information:

- Compliance and deployment information about key software updates
- Detailed state messages for the deployments and software update assets
- Error codes with additional information for software updates
- State messages for software update synchronizations
- Alerts for software update issues

Besides real-time information in the Configuration Manager 2012 console, you can also use the software update reports that are available out of the box.

Managing Superseded Software Updates In Configuration Manager 2007 software updates automatically expired after being superseded. This was done in the full software update synchronization process. You could not deploy superseded software updates because they were expired, and Configuration Manager 2007 doesn't allow you to deploy expired software updates.

Configuration Manager 2012 lets you choose to manage superseded software updates. You can also choose to configure a specific period of time in which the software update doesn't automatically expire after being superseded. This way you can deploy superseded software updates if necessary.

How to Manage Expired Updates

If software updates are expired, you can easily identify them and remove the membership of the software update groups. After you remove the membership, the maintenance cycle will remove the expired updates from the distribution points. This allows you to remove the expired updates from your distribution points in the Configuration Manager hierarchy.

Increased User Control over Installation of Software Updates The Empower Users pillar of Configuration Manager 2012 fits perfectly in the Software Updates feature. Configuration Manager 2012 allows users to have more control over when software updates are installed on their devices (Figure 9.1). Users can schedule or reschedule software installations or updates via the Software Center during non-working hours.

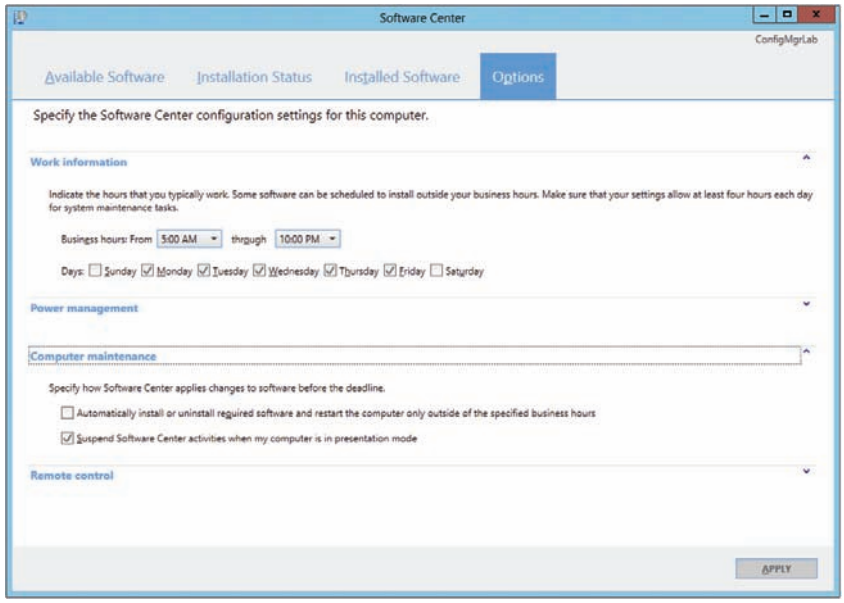


Figure 9.1 Defining business hours in the Software Center

Software Update Files Are Stored in the Content Library The content of software updates is also stored in the new content library of Configuration Manager 2012. The single-instance storage of the content library is also used for software updates. Before content files are downloaded, Configuration Manager 2012 checks to see if the content file is already in the content library. If the content file is available, it will use that file for the new software update.

Administrative Access Especially for the Software Update features, a role for software update management is defined in role-based administration. You can now delegate the deployment of software updates to your systems to the security officer, for instance. Or you can delegate it to a local administrator by limiting the scope of the role assignment.

Software Update Deployment Template Software update deployment templates could be created in the Configuration Manager 2007 console, but in Configuration Manager 2012 you can only create deployment templates with the Automatic Deployment Rules wizard or the Deploy Software Updates Wizard. The deployment template stores many of the deployment properties that will not change when you create new deployments.

Besides the new or enhanced features in the Software Updates feature, some others have been removed from Configuration Manager. Table 9.1 lists the removed features.

TABLE 9.1: Removed features

FEATURE	DESCRIPTION
Update lists	The update lists have been replaced by the new software update groups.
Deployments	Of course you can still deploy software updates. But now the deployment is nested in the software update group.

Prerequisites for Software Updates

Before you can plan and set up the Software Updates feature, you need to be familiar with its components, so you can determine which ones to install and configure for your environment. Table 9.2 provides a list of these components.

TABLE 9.2: External prerequisites to the Configuration Manager Software Updates feature

PREREQUISITE	DESCRIPTION
Windows Server Update Services (WSUS) 3.0 SP2 or later	Software Updates requires WSUS 3.0 or later to be installed before setting up the software update point site system role because it is used for update synchronization and compliance assessment on clients.
WSUS 3.0 Administrator Console or later	The WSUS 3.0 Administrator Console or later is required on the Configuration Manager site server when WSUS is not on the site server itself. The console is required in order to communicate with a remote WSUS server.

Prerequisite	Description
Windows Update Agent (WUA) 3.0 or later	The WUA 3.0 client or later is required, in addition to the Configuration Manager client, to connect to the WSUS server so it can retrieve the list of software updates that need to be scanned for.
Background Intelligent Transfer Service (BITS) 2.5	Microsoft highly recommends that BITS be enabled and configured for a Configuration Manager site and that distribution points also be BITS enabled. Because software updates are downloaded to the local client cache before they are installed, having BITS enabled will allow clients to continue a download of updates if a client is disconnected from a distribution point.
Windows Installer 3.1	Certain updates, such as ones for Microsoft Office, require Windows Installer 3.1 or they will not be detected during a scan for compliance. If you were using the ITMU tool for SMS 2003, this requirement has probably already been met.
Site server communication to the software update point (SUP)	There may be configuration settings that need to be examined depending on your software update point infrastructure and Configuration Manager settings. We will go into that in more detail in the section on planning the software update point installation.

Of course, you will also need to configure a SQL Reporting Services (SRS) reporting point before you can use the Software Updates reports. We'll go into more detail on configuring a reporting point in Chapter 13, "Reporting."

Elements of Software Updates

Before you can plan to implement the Software Update process, you need to become familiar with the various elements of the process and their roles in the overall picture.

Software Update Point

As discussed in Chapter 4, "Installation and Site Role Configuration," the *software update point* is a site system role that is required for managing software updates in Configuration Manager. Each Configuration Manager site must have at least one software update point that is able to synchronize with a source like Microsoft Update before it can deploy software updates to Configuration Manager clients. The software update point role can only be configured on a server that already has Windows Server Update Services (WSUS) 3.0 SP2 installed. The software update point software provides the bridge between the WSUS components and Configuration Manager. It allows synchronization with the WSUS database to download the latest software update information from Microsoft Update and locally published updates.

When the software update point site system role is created and configured as the software update point that synchronizes with a synchronization source, the software update point components are installed and enabled. The WSUS Control Manager component configures the associated WSUS server with the settings that were chosen when you set up the software update point site system role.

When you are deploying a Central Administration Site (CAS), you need to install the software update point in the CAS first.

The software update point settings can be changed from the Software Update Component Properties window via the Configuration Manager console:

1. Choose the System Center 2012 Configuration Manager console ➢ Administration ➢ Overview ➢ Site Configuration ➢ Sites.
2. Select the site for which you want to change properties.
3. Choose Configure Site Components ➢ software update point.

The software update point settings can modify the software update point site system server, the synchronization source, the schedule, and the products, classifications, and languages for which software updates will be synced with the database. You will find more details on these settings later in the chapter.

The first time the software update point completes its synchronization; the Software Updates client agent components are activated from a dormant state and will connect on a schedule to WSUS on the software update point server to start a scan for update scan compliance, as described earlier in the chapter.

Software Updates Agent

The Software Updates Agent is part of the Configuration Manager 2012 client. You can configure the Software Updates Agent with the client settings. With Configuration Manager 2012 you can create different client agent settings for groups of computers, so you are able to assign different settings for different groups of computers and servers. For instance, you can configure client settings for computers in such a way that all mandatory software updates that reach their deadline are installed immediately. For servers you can configure a different setting.

Software Updates Metadata

A software update has two parts: the software update file(s) and the metadata. The metadata is contained in the Configuration Manager database and provides information about the software update, including its name, description, products supported, update class, size, article ID, download URL, rules that apply, and so on.

Most important, the metadata for each software update defines what products are applicable to the update. A product (for example, Windows 7) is a specific edition of an OS or application. A product family (for example, Microsoft Windows) is a base OS or application from which single products come. You can select a product family or individual products when choosing what will be synced by Configuration Manager.

Multiple Product Updates

If an update is applicable to many products, and at least a few of those products from a product family have been chosen for synchronization, then all the updates will appear in the Configuration Manager console.

The metadata for each update also defines the update's *classification*. This represents the type of software an update will modify on clients. There can be many different classifications for any given product family, which we will go over in the "Planning to Use Software Updates in Configuration Manager" section of this chapter. The metadata also defines what languages the update file is applicable to, and it provides a summary of the software update in one or more languages.

Software Update Files

The software update files are the actual files that the client downloads, such as an `.exe`, a Windows Installer file (`.msi`), a Microsoft Update Standalone Package (`.msu`), or a Windows Installer patch (`.msp`), and then installs to update a component or application. The software update file might be stored on a WSUS 3.0 SP2 server that is configured to be a software update point, but it is always stored on distribution points for the site when the software update is downloaded or deployed. The process is as follows:

1. Software update files are retrieved from either the upstream server or Microsoft Update.

   An upstream server is a software update point higher in the Configuration Manager 2012 hierarchy.

2. The updates are then copied to distribution points when the software update is downloaded using the Download Software Updates Wizard or deployed to clients using the Deploy Software Updates Wizard.

   Both methods are covered in detail later in this chapter.

3. Both methods download the software update files to a temporary location on the site server hard drive.

4. The site server creates and stores a compressed package file containing the software update.

5. It decompresses the package file.

6. Then it copies the update file to the content library on the distribution point.

Software Update Objects

The Software Updates node in the Configuration Manager 2012 console is divided into four nodes, as shown in Figure 9.2.

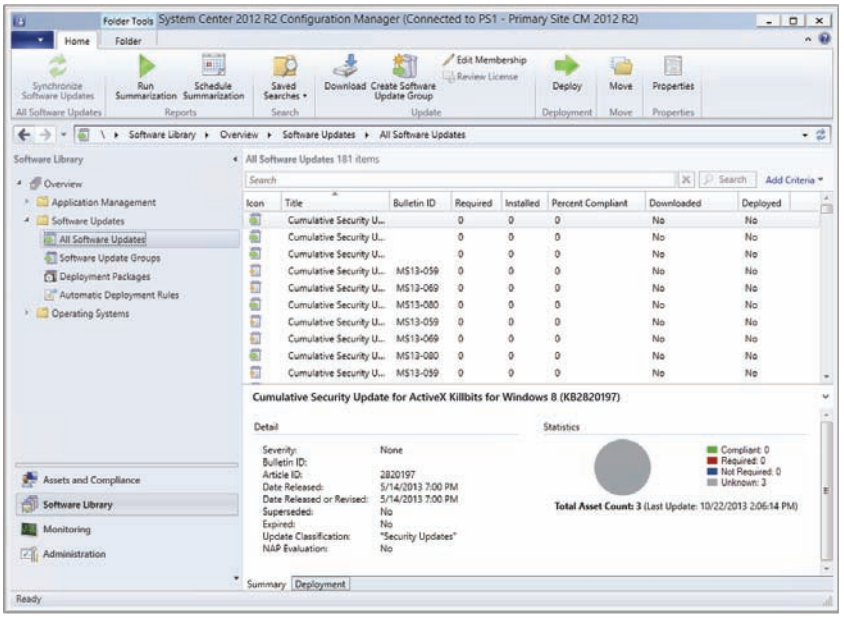


FIGURE 9.2 The Configuration Manager console showing the Software Updates node

In these nodes you will find the items that are related to the Software Updates feature. Table 9.3 lists the items that are related to Software Updates.

TABLE 9.3: Software Updates related items

OBJECT	DESCRIPTION
All Software Updates	Every software update has a configuration item object that is created during the software update sync cycle.
Software Update Groups	These are fixed sets of software updates that can be used for delegated administration and creating software update deployments.
Deployment Packages	These host the software update source files.
Automatic Deployment Rules	Automatic deployment rules give you the ability to automatically approve, download, and deploy software updates to all or a subset of your devices.
Deployment Template	This stores many of the deployment properties that may not change from one deployment to the next and are used to save time and ensure consistency when creating deployments. The deployment template is stored within the Configuration Manager database and is only accessible when creating a deployment or an automatic deployment rule.
Search	This feature provides an easy way to retrieve a set of software updates that meet the search criteria; the searches can be saved in the Configuration Manager database.

As noted in some of the preceding descriptions, software update deployment and deployment package objects are replicated from the site where they were created to all sites in the Configuration Manager hierarchy. The objects replicated to a child site will be read-only. Even though the properties for these objects must be modified at the site where they were created, the actions available for deployments at child sites are the same as those at the site where they were created. Also, deployment packages can be used to host the software updates that are deployed on the child sites.

Software Update Groups

A software update group in Configuration Manager contains a set of software updates. Software update groups offer several benefits for deploying and monitoring software updates and are part of Microsoft's recommended Software Updates workflow.

Using a software update group allows you to automate the process of approving and deploying software updates with automatic deployment rules. Tracking the compliance state for the software updates in deployments is an important task for Configuration Manager admins. If deployments are made without update groups, it's very hard to get the overall compliance state for the same set of software updates that have been sent out with multiple deployments. When update groups are used instead, you can use the Compliance 1 - Overall Compliance report for the set of updates in the software update group or the Compliance 3 - Update Group (Per Update) report to get a list of the updates in an update group and the overall compliance of each. This is a great reason to use software update groups as a part of your software update procedure.

Deployment Templates

Deployment templates can store many of the software update deployment properties, and they can be created for consistency, to save time, or to fit your software update procedures. You can create a deployment template in the process of creating a deployment or automatic deployment rule and save the settings in a template. Table 9.4 shows the deployment properties that are saved in a deployment template.

Table 9.4: Deployment template properties

Setting	Description
Collection	Indicates the collection that will be targeted for the software update deployment. This setting is optional when you make a deployment template.
Deployment Settings	Configured deployment settings such as Send Wake-up Packets or Verbosity Level are saved in the deployment template.
Deployment Schedule	Sets whether the user will be notified of pending updates, the installation progress for updates, whether the client evaluates the deployment schedule in local or Coordinated Universal Time (UTC), and the timeframe between when an update is available and when it is mandatory on clients.
User Experience	Hides software update installation and notifications. Sets the system restart behavior when an update installs on a client and needs to restart to finish. Also allows a system restart to be completed outside a maintenance window.

TABLE 9.4: Deployment template properties *(CONTINUED)*

SETTING	DESCRIPTION
Alerts	Sets if alerts are generated for the in-console alerting feature. Sets whether Operations Manager alerts are disabled while updates install and/or send an alert if the install fails.
Download Settings	Sets how clients will interact with the distribution points when they get a software update deployment.
Deployment Location	Sets whether to download the software updates from the Internet or a network file share.
Language Settings	Sets the language of the software updates that need to be downloaded and deployed.

Creating deployment templates in advance for typical deployment scenarios in your environment allows you to create deployments using templates that populate many of the properties that are most often static for the particular deployment scenario. Using the deployment template also reduces the number of wizard pages to work through in the Deploy Software Updates Wizard by up to seven pages, depending on what information you have already populated. This not only saves time but also helps to prevent mistakes when setting up a deployment.

Deployment Packages

A *deployment package* is the method used to download software updates (either one or several) to a network shared folder, which must be manually created before it is used, and copy the software updates source file to distribution points defined in the deployment.

Software updates can be downloaded and added to deployment packages prior to deploying them by using the Download Software Updates Wizard. This wizard provides admins with the capability to provision software updates on distribution points and verify that this part of the deployment process works properly.

When downloaded software updates are deployed using the Deploy Software Updates Wizard, the deployment automatically uses the deployment package that contains each software update. When software updates are selected that haven't been downloaded or deployed, a new or existing deployment package must be specified in the Deploy Software Updates Wizard, and the updates are downloaded to the package when the wizard is finished.

There is no hard link between a deployment and a specific deployment package. Clients will install software updates in a deployment by using any distribution point that has the software updates, regardless of the deployment package. Even if a deployment package is deleted for an active deployment, clients will still be able to install the software updates in the deployment—as long as each update has been defined in at least one other deployment package and is present on a distribution point that the client can get to. To help prevent software update deployment failures, you should make sure that deployment packages are sent to a group of distribution points that can be accessed by all the clients you are targeting.

Deployment package access accounts allow you to set permissions to specify users and user groups who can access a deployment package folder on distribution points. Configuration Manager makes these folders available to everyone by default, but you can modify this access if required for a specific security need.

Configuration Manager 2012 client computers also have the option of selective download: A deployment package might contain both updates that are required for a client and some that are not, but the client can determine which software updates are applicable and retrieve only those files. This allows admins to have multiple updates in a single deployment package and use it to target clients that might need only some of those updates.

Deployments

While it is deployment packages that host the update files, it is *software update deployments* that actually deliver software updates to clients. The Deploy Software Updates Wizard is used to create deployments and can be started using several methods, which we will detail later in the chapter. Table 9.5 lists all the pages in this wizard and describes the settings that can be configured in each one to create a software update deployment.

Table 9.5: Deploy Software Updates Wizard settings

Page	Description
General	Provides the name of and comments about the deployment; the update or update group and collection also need to be supplied.
Deployment Settings	Defines if the deployment is required or optional and sets the verbosity level. Also configures whether to send wake-up packets.
Scheduling	Sets whether the user will be notified of pending updates and/or the installation progress for updates, if the client evaluates the deployment schedule in local or Coordinated Universal Time, and the timeframe between when an update is available and when it is mandatory on clients.
User Experience	Defines if users will receive notice of installations of software updates and what happens when an installation deadline is reached. Defines the system restart behavior when an update installs on a client and needs to restart to finish. Defines if the Windows Embedded write filter is enabled or bypassed for this deployment.
Alerts	Sets the in-console alert handling of Configuration Manager and sets if System Center Operations Manager (SCOM) alerts are disabled while updates install and whether to send an alert if the install fails.
Download Settings	Sets how clients will interact with the distribution points when they get a software update deployment. Defines whether clients should use Microsoft Updates for content download if the updates are not present on the preferred distribution point, or whether to download software updates content when on a metered Internet connection.
Deployment Package	Shows the deployment package that will host the software updates for the deployment. This setting won't appear if the updates have already been downloaded to a package.
Download Location	Lets you choose to download the updates from the Internet or from a source on the local network.
Languages Selection	Lets you select the languages for which the software updates that will be in the deployment are downloaded.

If an update in a deployment has Microsoft Software License Terms that have not been accepted yet, then a Review/Accept License Terms dialog box will appear before the Deploy Software Updates Wizard and give you a chance to review and accept the license terms. When you accept the terms, then you can deploy the updates. If you don't accept the terms, the process is canceled.

Automatic Deployment Rules

A new Software Updates feature in Configuration Manager 2012 is Automatic Deployment Rules. This feature lets you define rules for specific types of software updates that can be downloaded and added to a software update group automatically. If a software update group is enabled for deployment, the updates are automatically deployed to your workstations. The Automatic Deployment Rules feature can be used for two common scenarios, namely:

- Automatically deploying Endpoint Protection definition and engine updates
- Patch Tuesday security patches

For both scenarios two out of the box templates are available to assist you in creating the automatic deployment rules. When you create an automatic deployment rule, you need to define whether you want to add the updates to an existing software update group or to automatically create a software update group.

When you deploy Endpoint Protection (System Center Endpoint Protection) definition and engine updates, you can add these updates to an existing software update group. The reason for this is that only four definition updates are available per agent for Endpoint Protection. Three of them are superseded, and only one is active. Every fifth definition update will be expired and fall out of the software update group. Configuration Manager 2012 R2 is able to run the automatic deployment rule up to three times a day, in line with the definition updates publishing frequency.

If you want to deploy the Tuesday patches automatically, it is recommended that you create a new software update group every Patch Tuesday. This keeps your software updates organized.

You can automatically select software updates based on the following parameters:

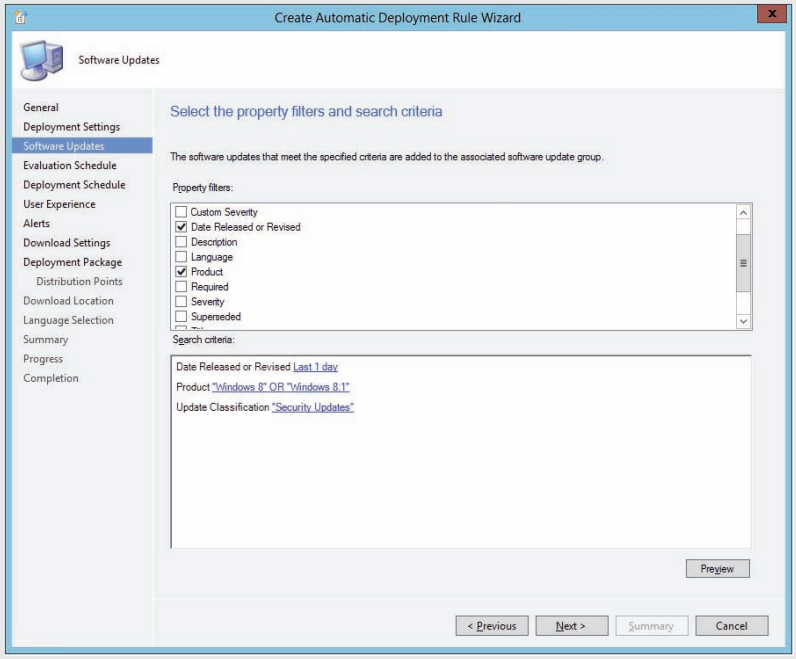
- Article ID
- Bulletin ID
- Custom severity
- Date released or revised
- Description
- Language
- Product
- Required
- Severity
- Superseded
- Title
- Update classification
- Vendor

Running an automatic deployment rule for a longer time can result in a very large package size. You are able to change the deployment package in an automatic deployment rule to limit the size of the package.

Automatic Deployment of Patch Tuesday Software Updates

The Automatic Deployment Rules feature allows you to automate the deployment of software updates. You can use it to automatically deploy the Patch Tuesday software updates for test purposes or prepare the deployment in production. Depending on your requirements, you can configure an automatic deployment rule for Windows 8 or 8.1 Patch Tuesday updates by creating an automatic deployment rule with the following steps:

1. Create a new software update group each time the rule runs. This way you are able to group the update groups per Patch Tuesday cycle, and you will limit the size of the software update deployment.
2. Select Enable The Deployment after this rule has run.
3. Select a collection with your test systems where you want to automatically test the Patch Tuesday patches.
4. Supply the following search criteria for the rule:
   - Product: Windows 8 OR Windows 8.1
   - Date Released Or Revised: Last 1 Day
   - Update Classification: Security Updates



5. Before going further, preview the number of updates that will be initially discovered. This way you can test your criteria before going into production and, for instance, accidently automatically deploying hundreds of updates.
6. Evaluation Schedule: Be sure the evaluation runs after the Software Update Synchronization Schedule on the second Tuesday of every month.
7. Deployment Schedule: Enable the availability of the deployment for four hours after the deployment is created so that you are sure that the deployment has been distributed throughout your Configuration Manager hierarchy. Configure whether you want the deadline for the deployment.

After you configure the rest of the automatic deployment rule, the rule will create a software update deployment every second Tuesday of the month.

System Center Updates Publisher

The System Center Updates Publisher was built on the custom updates framework that was introduced in Systems Management Server 2003 R2. Updates Publisher is a stand-alone tool that enables independent software vendors or line-of-business developers to import custom software update catalogs, create and modify software update definitions, export update definitions to catalogs, and publish software update information to a configured WSUS server. By using Updates Publisher to define software updates and publish them to the WSUS server, the Software Updates feature in Configuration Manager is able to synchronize the custom update from the WSUS server database to the site server database. This will allow you to enable client computers to scan for custom update compliance and to provide administrators with the ability to deploy the custom updates to client computers.

The Software Update Process in Configuration Manager

As you'll see throughout the hands-on portions of this chapter, the biggest parts of the software update process are planning and configuration. After you've completed those, Configuration Manager itself performs three main operational phases: synchronization, scanning for compliance, and deployment.

Synchronization

Synchronization is the process of retrieving the metadata for software updates that meet the configured criteria; it can be retrieved from either the upstream Windows Server Update Services (WSUS) 3.0 SP2 server or Microsoft Update. The WSUS Synchronization Manager component on the software update point works with WSUS to complete the synchronization process. The highest site (Central Administration Site) in the Configuration Manager hierarchy that has a software update point synchronizes with, for instance, Microsoft Update; this is done either on a schedule you set up or manually by using the Synchronize Software Updates action on the All Software Updates node in the Configuration Manager console. (We go into more detail on how to do that later in the chapter.) When a sync cycle is started at the CAS, the WSUS Synchronization Manager makes a request to the WSUS service to start a sync cycle. The software update's metadata is then synchronized from Microsoft Update, and any changes are inserted into the WSUS database.

When WSUS finishes its sync cycle, WSUS Synchronization Manager starts syncing with the WSUS database and inserts any changes into the site server database. When that process is finished, the WSUS Synchronization Manager component (SMS_WSUS_SYNC_MANAGER) creates a status message with an ID of 6702.

Difference between Scheduled and Manual Synchronization

A scheduled synchronization does a full sync, but the Run Synchronization action does only a delta sync. Updates are marked as expired if they are superseded by another software update or marked as expired in the update catalog. They are marked as expired only during the scheduled synchronization.

When a sync is run on a schedule, all changes to the software update metadata since the last scheduled sync are put into the site database. This includes metadata that is new (products, languages, and so on), modified, or removed. A manually run sync will be faster than a scheduled one because it downloads only delta changes to what already exists in the database.

When a software update sync finishes at the CAS, a sync request is sent out to all of its child sites. When a child site gets that request, it will first sync itself from its parent site and then send out a request to any child sites that are configured as software update points. This continues on down the hierarchy until all child sites have been synchronized.

With an Internet-based software update point (which is also used in Network Access Protection scenarios), a sync request is sent to it right after the software update point that synchronizes with the synchronization source is finished with its syncing request. The process for both is the same except that the upstream server of the Internet-based software update point is automatically configured to be the first software update point for the site, and the site server database is not updated when the Internet-based software update point finishes its sync cycle.

If the synchronization fails, there is a retry interval of 60 minutes. The WSUS Synchronization Manager component will schedule the sync to run again 60 minutes after the process fails and start over. WSUS Synchronization Manager will create a status message with an ID of 6703 in the case of a sync failure.

Compliance

When software update synchronization completes at each site, a sitewide machine policy is created that allows client computers to retrieve the location of the WSUS server and to start a scan for software update compliance. When a client receives that machine policy, a compliance assessment scan is scheduled to start at a random time within the next two hours. When the scan runs, a component of the client Software Updates Agent clears the previous scan history, sends a request to find the WSUS server that should be used for the scan, and then updates the local Group Policy with the WSUS server location.

The scan request is then passed to the Windows Update Agent (WUA). The WUA then connects to the WSUS server that it just got information about, downloads a list of the software updates that have been synced with the WSUS server, and scans the client computer for the updates in the list. A component of the Software Updates Agent then sees that the scan for compliance is finished and sends a state message for each software update that had a change in compliance

state since the last scan. Those state messages are then sent to the client's management point in bulk every five minutes. The management point will then forward the state messages to the site server, where they are inserted into the site server database.

Supersedence occurs when a new software update has the same fixes as a previous update but may have fixed issues with the update and/or added new fixes. In SMS 2003, when new software updates supersede ones that had the same fixes, they may both be marked as needed when only the new one is necessary. In Configuration Manager 2012 Software Updates, you can now configure the supersedence behavior; you can either choose to expire a superseded update or choose to expire the update after a configurable number of months at the software update point. When new software updates are released that supersede others, Microsoft Update is refreshed with that information. When client computers are scanned for compliance, the new updates produce a compliance state by the client, but the older updates do not. The only time this is not the case is when a service pack contains a required update. The WUA will then return a compliance state on both, which allows admins to deploy individual updates or service packs as needed. Table 9.6 shows details on the four states of compliance for Software Updates.

TABLE 9.6: Software Updates compliance states

STATE	DESCRIPTION
Required	The software update is applicable to the client, which means any of the following conditions could be true: ◆ The update has not been deployed to the client. ◆ The update has been installed, but the state of the update hasn't been updated in the database yet. ◆ The update has been installed, but the client requires a reboot before it finishes. ◆ The update has been deployed but is not yet installed.
Not Required	The update isn't applicable on the client.
Installed	The update is applicable on the client, and it has already been installed.
Unknown	This state usually means that the software update has been synced to the site server, but the client hasn't been scanned for compliance for that update.

Deployment

The compliance assessment data is then used to determine which software updates are required on client computers. When you create a software update deployment with the Deploy Software Updates Wizard, as described later in this chapter, the software updates in the deployment are downloaded from the location specified on the Download Location page of the wizard to the configured package source, if they haven't been downloaded already. When the wizard finishes, a deployment policy is added to the machine policy for the site. The updates are then copied from the package source to the shared folders on the distribution points set up in the package, where they will be available for clients.

When a client in the target collection of the deployment receives the machine policy, the software update client component starts an evaluation scan. Updates that are still required on the client are then added to a class in Windows Management Instrumentation (WMI). Any updates that are mandatory deployments are downloaded as soon as possible from the distribution point to the local cache on the client. The updates in the optional deployment category are not downloaded until they are manually started. If an optional deployment has a deadline that makes it mandatory, the client will download the update as soon as it registers the change in deployment status.

Software Updates in Configuration Manager Are Always Downloaded to the Client

Software updates are always downloaded to the local client cache before they are run in Configuration Manager. You no longer have the option to have them run from a distribution point as you did in SMS 2003.

If the client can't find the location of the distribution point through Location Services (via requests of the management point), it will keep trying to find a distribution point for up to 5 days before it stops. If the client can't connect to the distribution point to which it has been referred as a source of the software updates in order to download the updates, it will try for up to 10 days before it stops trying. When you start updates manually, the client will try every hour for each distribution point for up to 4 hours before it fails.

When an update deployment has a deadline that becomes available for deployment on a client, the Available Software Update icon will show up in the notification area to tell a user that the deadline is coming up. By default, these display notifications will show up on a periodic basis until all mandatory updates have been installed. They will be displayed every 48 hours for deadlines more than 24 hours away, every 4 hours for deadlines less than 24 hours away, and every 15 minutes for deadlines less than an hour away.

Just imagine the phone calls you'd get if you left things that way! Fortunately, Microsoft has given you the option to turn these notifications off with the client agent settings that let you hide all software update deployments from users. This setting doesn't affect regular Software Deployment settings, but it will keep display notifications, notification area icons, and software update installation progress boxes from appearing at all. However, this will also mean that you can send out only mandatory software update deployments to your clients. We recommend doing this anyway because users will more than likely delay deployments until they become mandatory.

Unless you hide your update deployments, users will be able to open the Express/Advanced dialog box to start up the installation of all mandatory software updates at once. They will also be able to open the Available Software Updates dialog box, where they can choose to install whatever is available.

When the deadline passes on a mandatory update, a scan will start on the client to make sure that the updates are still required; the local client cache will be checked to make sure the updates are still available, and then the updates will be started. When that is done, another scan will start to make sure that the updates are no longer required on the client. Finally, a state message is sent to the management point saying that the updates are now installed.

Limit of 1,000 Software Updates in a Deployment

Be sure to limit the number of software updates in your Software Updates Deployments. Configuration Manager 2012 supports up to 1,000 software updates per deployment. When using automatic deployment rules, be sure that the criteria you use will not return more than 1,000 software updates as a result.

Planning to Use Software Updates in Configuration Manager

Now that you have seen what is new in Configuration Manager Software Updates, the prerequisites, and the major components of the process, you can plan the use of Software Updates in your environment.

To plan the implementation of Software Updates in Configuration Manager, you can use the same process of deployment intelligence that we used to plan the deployment of Configuration Manager itself in Chapter 2, "Planning a Configuration Manager Infrastructure." Using this method will help you ensure that you get everything out of Software Update that your company requires to keep your computer resources up to date with the latest software upgrades and patches.

Deployment intelligence for Software Updates has three parts:

- Determine what needs to be accomplished with Software Updates.
- Determine what is on the network now and what has been used in the past.
- Test in an isolated lab.

Determining What Needs to Be Accomplished

This may seem like a no-brainer, because the first thing that probably comes to mind is "deploy patches," but with Configuration Manager you can do a lot more than just deploy security patches, as you will soon learn.

This part of the planning will also let you decide how you want to configure your test environment, your Software Update point infrastructure, and the settings for the Software Update servers and client agent.

Planning for Software Update Point Infrastructure

Software update points can be used in a hierarchy or in stand-alone sites. In both cases you need to plan the placement of the software update point. Determine whether you need more than one software update point in a site.

Planning Software Update Points in a Hierarchy

When you have a Configuration Manager 2012 hierarchy, the Central Administration Site server is at the top of the Configuration Manager hierarchy. One software update point is configured on the Central Administration Site so that software updates can be managed. Most of the synchronization settings are configured there and propagated down to the rest of the sites in the hierarchy. The software update point on the Central Administration Site is what syncs

with Microsoft Update or another upstream WSUS server. The software update points in the primary sites that are children of the Central Administration Site are automatically configured to synchronize with the software update point in the Central Administration Site.

When using a software update point in a primary site with secondary sites, the child sites sync with the software update point that is set up on the parent site. Secondary sites can be set up with a software update point, or clients at the secondary site can connect directly to the software update point on the parent primary site.

Planning a Software Update Point in a Stand-Alone Primary Site

When you have only a single primary site, the software update point needs to be configured on the primary site server, and it will sync with Microsoft Update or another upstream WSUS server.

Planning to Add More Than One Software Update Point per Primary Site

With Configuration Manager 2012 R2 you are able to install more than one software update point per primary site. When installing more than one software update point in your primary site, you can create a form of high availability for deploying software updates. By adding software updates points, you provide the ability for clients to switch between software update points when one is unavailable. Switching software update points is based on a software update point list; this list allows the client to randomly select a software update point when the configured software update point is not available. Configuration Manager can provide a client with a different list, depending on the type of client:

Intranet-Based Clients Intranet-based clients will receive a list of software update points that are configured to allow connections from the intranet only combined with those that allow connections from the Internet and intranet.

Internet-Based Clients Internet-based clients will receive a list of software update points that are configured to allow connections from the Internet only combined with those that allow connections from the Internet and intranet.

The software update points that are in the same Active Directory forest are prioritized above the ones that are not in the same forest but are part of the same Configuration Manager infrastructure.

When using software update point switching, keep the following in mind. When a client is assigned to one software update point, it stays assigned to this software update point until it fails and becomes unavailable. Then the client will automatically connect to a different software update point. It stays assigned to this new software update point until it fails and becomes unavailable, even if the first software update point becomes available again. The following process is used to switch a software update point:

1. When an initiated or scheduled software update scan fails, the client waits 30 minutes and retries the scan using the same software update point.
2. After the scan fails four times at an interval of 30 minutes (2 hours total), the clients waits another 2 minutes before switching to another software update point based on the software update point list.
3. When the software update scan is successful, the client will be connected to the new software update point going forward.

When using this default method in a large environment and one software update point becomes unavailable for a longer time, all clients will be connected to one software update point. This may cause unnecessary extra load on the software update point. Another, better way is using Network Load Balancing (NLB); this way the clients will connect to the virtual IP address of the Network Load Balancer instead of directly to the site server.

If you are going to have more than 25,000 clients connecting to WSUS on a software update point, a NLB cluster must be configured on the WSUS server and then configured for the Configuration Manager site so that the NLB cluster is used as the software update point.

Enable Network Load Balancing for a Software Update Point

Enabling Network Load Balancing awareness for software update points cannot be done from the Configuration Manager 2012 R2 console. To be able to do this, you need to use PowerShell to set up NLB.

When you want to enable NLB for software update points at site servers CM01 and CM02, you need to use the following PowerShell command to configure it:

```
Set-CMSoftwareUpdatePoint -NlbVirtualIP SUP.CONFIGMGRLAB.COM
-SiteSystemServerName CM01.CONFIGMGRLAB.COM -SiteCode PS1
Set-CMSoftwareUpdatePoint -NlbVritualIP SUP.CONFIGMGRLAB.COM
-SiteSystemServerName CM02.CONFIGMGRLAB.COM -SiteCode PS1
```

Planning for Internet

When your site is in secure (HTTPS) mode, you have the option to configure a software update point to accept connections from clients on both the intranet and the Internet, from only clients on the intranet, or from only clients on the Internet. When Internet-based client connectivity is not accepted on the primary software update point used for clients in the intranet, you can set up separate Internet-based software update points if needed.

This site system server role must be assigned to a site system server that is remote from the site server and the software update point. When the Internet-based software update point doesn't have connectivity to the first software update point for the site, you will have to use the export and import functions of the WSUSUtil tool to sync the software update metadata.

Planning for the Software Update Point Install

Before setting up the software update point site system role in Configuration Manager, you must consider several requirements depending on your Configuration Manager infrastructure, such as when the software update point will be configured to communicate using SSL, or when the site server is in secure mode, and so on. You must take additional steps before the software update point in the hierarchy will work properly.

As discussed earlier in the chapter, Software Updates requires that Windows Server Update Services 3.0 SP2 be installed on all site systems servers that will be configured for the software update point site system role. There can be many site systems with the software update point role, but only one site system can be configured as the software update point. Also, when the software update point is not on the site server itself, the WSUS 3.0 SP2 administrative console is

required on the site server, which lets the site server communicate with the WSUS components on the software update point. You can configure an account to connect to a remote WSUS server or a WSUS server in another forest. If you are going to use an NLB cluster, the full install of WSUS 3.0 SP2 is required on all site systems that will be in the cluster.

During the WSUS install, you can choose to use the default or a custom website to host the WSUS components. If WSUS is going to be installed on a primary Configuration Manager site system, Microsoft recommends that you choose a custom website so that IIS hosts the WSUS 3.0 SP2 services in a dedicated website instead of sharing the site with Configuration Manager site systems or other applications.

You can use a WSUS server that was active in your environment before Configuration Manager was implemented. When the WSUS server is configured as the first software update point, the sync settings are then specified. All of the software update metadata from the WSUS server will be synced to the Configuration Manager database regardless of the sync settings for the software update point. Be sure to disable the Group Policies that point the clients to the WSUS server.

When your Configuration Manager site server is in secure mode or when the software update point is configured to use SSL, a web server certificate must be assigned to the website used by WSUS. When you use a custom website for WSUS, per Microsoft's recommendation, the WSUS website must be assigned a web server certificate where the Subject Name or Subject Alternate Name field contains the Internet fully qualified domain name (FQDN). The upstream WSUS server must be set with the same certificate, or SSL communication will fail between the servers. The certificate must also reside in Trusted Root Certification Authorities in the Computer certificate store on each client computer, or it will fail to scan for software update compliance.

When the site server is in secure mode, the web server certificate that is used for the Configuration Manager site systems can also be used by the WSUS website. Also, when the WSUS uses the same website as the Configuration Manager site server, and the site is in secure mode, the default website might already be assigned the right web server certificate. The certificate would still need to be configured on the upstream WSUS server, but it should already be configured on Configuration Manager clients.

If there is a firewall between the Configuration Manager software update point and the Internet, a software update point and its upstream server, or an Internet-based software update point and the software update point for the site, the firewall might have to be configured to accept the HTTP and HTTPS ports used for the WSUS website. By default, a WSUS server that is configured for the default website uses port 80 for HTTP and 443 for HTTPS communication, while one configured for a custom website uses port 8530 for HTTP and 8531 for HTTPS communication.

If your company doesn't allow these ports and protocols to be open for all addresses on the firewall between the software update point and the Internet, you can restrict access to the following URLs so that WSUS and Automatic Updates can communicate with Microsoft Update.

```
http://windowsupdate.microsoft.com

http://*.windowsupdate.microsoft.com

https://*.windowsupdate.microsoft.com
```

```
http://*.update.microsoft.com

https://*.update.microsoft.com

http://*.windowsupdate.com

http://download.windowsupdate.com

http://download.microsoft.com

http://*.download.windowsupdate.com

http://test.stats.update.microsoft.com

http://ntservicepack.microsoft.com
```

If there is an Internet-based software update point, or there are child sites with a software update point, these addresses might also need to be added to a firewall between the servers:

```
http://<FQDN for software update point on child site>

https://<FQDN for software update point on child site>

http://<FQDN for software update point on parent site>

https://<FQDN for software update point on parent site>
```

Planning the Software Update Server Settings

There are software update point settings and general site settings that have an impact on software updates in Configuration Manager. These settings configure the first software update point and determine which updates are synchronized, whether there are maintenance windows for installing updates, how much time software updates have to complete, and so on.

The software update point settings configure which site system server is the software update point that is used to synchronize with Microsoft Update or another source. You can also configure which site system server is the Internet-based software update point if one is specified at the site, the sync source, the sync schedule, the products, the classifications, and the languages for which software updates will be synchronized. After starting the Add Site Systems Roles Wizard, you will be faced with several decisions to make about how you want the software update point configured for your environment.

General Settings

At the general settings page you are able to set which ports and, if needed, which proxy server and proxy-account are used.

Software Update Point This setting will determine which ports are used for connectivity to the site system server that is assigned the software update point role and whether SSL is

used when synchronizing data from the software update point and when clients connect to the WSUS server on the software update point. Ports 80 and 443 are set as the default for client communications, and SSL is not set by default.

Proxy and Account Settings If a proxy server will be required by your environment in order to synchronize this software update point, you will have the opportunity to determine whether to use a proxy server for synchronizing software updates, to use a proxy server to download content using an automatic deployment rule, or both. You will also be able to specify alternate credentials in order to make authenticated connections from the site to the WSUS server if desired.

Synchronization Settings

The sync settings for the software update point specify the sync source and whether WSUS reporting events are created during the sync process.

Synchronization Source The sync source for the first software update point at the central site is configured to use Microsoft Update, but it can be changed to use a custom upstream data source location (URL), or you can choose not to synchronize with any of the two sources. The software update point on child sites is automatically configured to use the software update point on its parent site as the sync source. When there is an Internet-based software update point, the software update point for the site is automatically set to be the sync source. When you choose not to sync with a sync source, you can use the export and import functions of the WSUSUtil tool instead to get the updates you need.

WSUS Reporting Events The Windows Update Agent on clients can create event messages that are used for WSUS reporting. These events are not used in Configuration Manager, so the Do Not Create WSUS Reporting Events setting is checked by default. When these events are not created, the only time clients should connect to the WSUS server is during software update evaluation and compliance scans. If these events are needed outside of the Configuration Manager reporting for software updates for some reason, then you will need to modify this setting for your specific needs.

Synchronization Schedule The sync schedule can be configured only at the software update point on the central Configuration Manager site (Central Administration Site or stand-alone primary site). When this schedule is configured, the software update point on the central site will start syncing with the configured synchronization source at the scheduled date and time. The custom schedule allows you to sync software updates on a date and time when the demands from the WSUS server, site server, and the network are low and less likely to interfere with regular network traffic. You can also run a sync cycle manually from the central site from the Update Repository using the Run Synchronization action in the Configuration Manager console.

After the software update point successfully syncs with the synchronization source, a sync request is sent to the Internet-based software update point, if there is one, and to the software update point on child sites. This process repeats throughout the hierarchy until it is successful.

Supersedence Rules You can configure a software update to expire as soon as it is superseded by a more recent software update. You also can set an update to expire that is superseded after a specific period of time. Supersedence settings are not applicable for

System Center endpoint definition updates. Definition files are automatically expired after four newer definition updates are released. Supersedence settings are also not applicable for software updates that are superseded by a service pack; these software updates will never expire after they are superseded.

Update Classifications Updates are defined with classifications that help to organize the different types of updates. During the sync process, the software updates metadata for the specified classification will be synchronized. Table 9.7 shows the classifications of updates that can be synced with Configuration Manager.

TABLE 9.7: Update classes

Update Class	Description
Critical updates	Broadly released fixes for specific problems addressing bugs that are critical but not security related.
Definition updates	Updates to virus or other definition files.
Feature packs	Feature packs will often bring more functionality to a product; they are also deployed via software updates.
Security updates	Broadly released fixes for specific products, addressing security issues.
Service packs	Cumulative sets of all hotfixes, security updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.
Tools	Utilities of features that aid in accomplishing a task or set of tasks.
Update rollups	Cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component, such as IIS.
Updates	Broadly released fixes for specific problems addressing non-critical, non–security-related bugs.

You will need to decide if you are going to deploy some or all of these categories or even pick and choose specific updates from each category in your environment. The update classification settings are configured only on the highest software update point in the Configuration Manager hierarchy. They are not configured anywhere else because they synchronize the metadata from the upstream sync source using the class settings from the central site. When you choose update classes to sync, remember that the more classes you choose, the longer it will take to sync the software update metadata.

Products The metadata for each update sets the product or products for which the update is applicable. A product is a specific edition of an operating system (such as Windows 8) or application, while a product family is the base operating system or application to which the

individual products belong (such as Microsoft Windows). You can choose a product family or individual products within a product family.

When updates are applicable to several products and at least one of the products is one you have chosen to update, all of the products will appear in the Configuration Manager console even if they haven't been selected.

The Products settings, like other software update settings, are configured only on the software update point highest in the Configuration Manager hierarchy.

Languages This setting allows you to configure the languages for which the summary details will be synced for a software update and the update file languages that will be downloaded for the software update.

Software Update File The languages configured for the Software Update File setting provide the default set of languages that will be available when downloading updates at the site server. When you're on the Language page of the Deploy Software Updates Wizard or Download Software Updates Wizard, the languages configured for the first software update point are automatically selected, but they can be modified each time updates are downloaded or deployed. When the wizard finishes, the software update files for the configured languages are downloaded, if they are available, to the deployment package source location and copied to the distribution points configured for the package.

The Software Update File language settings should be configured with the languages that are most often used in your environment. For example, if your clients use English and Spanish for the operating systems or applications and not much else, then select those languages in the Software Update File column and clear the others. This will allow you to use the default settings on the Language Selection page of the wizards most of the time, and it also prevents unneeded update files from being downloaded. This setting is configured at each software update point in the Configuration Manager hierarchy.

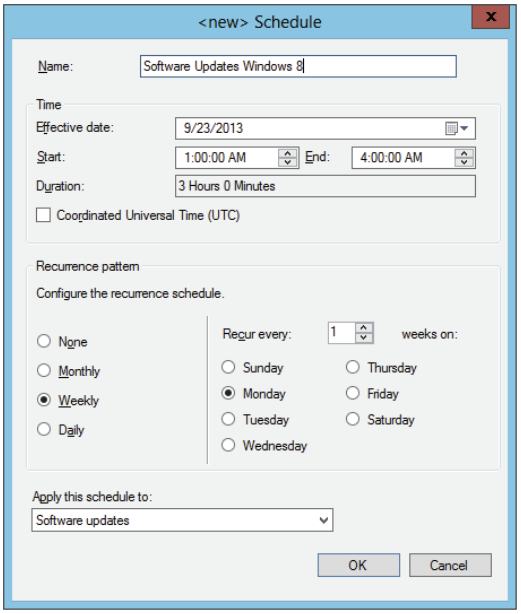
Summary Details During the sync process, the Summary Details information (Software Update metadata) is updated for the languages selected. The metadata provides information about the software update, such as name, description, products supported, update class, article ID, download URL, applicability rules, and so on.

When selecting the Summary Details languages, you should select only the languages needed in your environment. The more languages that are selected, the longer it will take to sync the Software Update metadata. The metadata is displayed in the location of the operating system where the Configuration Manager console is running. If localized properties for the software are not available, the information displays in English.

Maintenance Windows

Maintenance windows provide admins with a way to define a period of time that limits when changes can be made on the systems that are members of a collection. Maintenance windows restrict when the software updates in deployments can be installed on client computers, as well as restrict operating system and software distribution deployments. In Configuration Manager 2012 R2 you can create maintenance windows that apply specifically to software updates, as shown in Figure 9.3. This way you are able to create more granular maintenance windows for software updates that may have a higher priority, for instance, than an application deployment. You can create more than one maintenance window.

FIGURE 9.3
Creating a maintenance window



Client computers determine whether there is enough time to start a software update install through the following settings:

Restart Countdown The length of the client restart notification (in minutes) for computers in the site. The default interval is 15 minutes, and it is a global site setting that can be changed in the Client Settings dialog box, in the Computer Restart setting.

System Restart Turnaround Time The length of time given for computers to restart and reload the operating system. This setting is in the site control image and has a default of 10 minutes.

Maximum Run Time The amount of time estimated for a software update to install on a client. The default is 10 minutes for updates and 60 minutes for a service pack. This timeframe can be changed for each software update on the Maximum Run Time tab of the properties of a software update.

When you use these setting to determine the available time in a maintenance window, each software update has a default of 35 minutes. For service packs, the default is 85 minutes. When you plan for maintenance windows in your deployments, take these defaults into consideration. When planning software update deployments, be aware of the collection's maintenance window and how many updates are in a deployment so that you can calculate whether clients will be able to install all the updates within the maintenance window or the installation of updates will span multiple maintenance windows.

When a software update installation completes but there is not enough time left in the maintenance window for a restart, the computer will wait until the next maintenance window and restart before starting any more update installs.

If more than one update is to be installed on a client during a maintenance window, the update with the lowest maximum run time installs first, then the next lowest installs, and so on. Before installing each update, the client will verify that the available maintenance window is long enough to install the update. Once an update starts installing, it will continue to install even if the install goes beyond the maintenance window.

When you create a software update deployment, there are two settings that can allow maintenance windows to be ignored:

Deadline Behavior - System Restart (If Necessary) You can set this option to indicate whether you want to allow system restarts outside configured maintenance windows. By default, this setting is disabled. This setting comes in handy when you want your software update install to complete on clients as soon as possible. When this setting is not enabled, a system restart will not be triggered if the maintenance window ends in 10 minutes or less. This could prevent the install from completing and leave the client in a vulnerable state until the next maintenance window. This setting is available on the User Experience page of the Create Automatic Deployment Rule Wizard or the Deploy Software Updates Wizard.

Deadline Behavior - Software Updates Installation This setting determines whether software updates in the deployment are installed at the deadline regardless of a configured maintenance window. It is disabled by default. This setting comes in handy when you have software updates that must be installed on clients as soon as possible, such as security patches to fix a vulnerability that is being exploited on the Internet. This setting is available on the User Experience page of the Create Automatic Deployment Rule Wizard or the Deploy Software Updates Wizard.

Software Update Properties

Each software update has a properties box with tabs that provide configuration settings to enable software updates and configure the update settings on clients:

Maximum Run Time Tab This tab allows you to set the maximum amount of time a software update has to complete installing on clients, in minutes. If the maximum runtime value has been reached, a status messages is created and the deployment is no longer monitored. This setting is also used to determine whether the update should be started within a configured maintenance window. If the maximum runtime value is greater than the time left in the maintenance window, the software update installation is not initiated until the start of the next maintenance window.

Keep in mind that if a maximum runtime value is set for more time than the configured maintenance window of a collection it targets, it will never run on those clients. This setting can be configured only on the site synchronized with Microsoft Update, which is more than likely the Central Administration Site, and the default is 60 minutes for service packs and 10 minutes for all other types. Values can range from 5 to 9,999 minutes.

Custom Severity Tab This is a nice addition to Software Updates that allows you to assign custom severity values for software updates if the default value doesn't meet your organization's needs. The custom values are listed in the Custom Severity column in the Configuration Manager console. The software updates can be sorted by custom severity values, the search

criteria can be created based on these values, and queries and reports can be made that filter on these values—whatever suits your needs. This setting can be configured only on the site that syncs with Microsoft Update.

Planning for Software Updates Client Settings

The Software Updates client settings in Configuration Manager can be configured sitewide (by default), and you can configure client settings for specific collections. There are Software Updates client agent settings and general settings that affect when updates are scanned for compliance and how and when updates are installed on clients. The client agent settings specific to software updates are configured in the Software Updates Client Agent properties, and the sitewide general or collection-based settings related to software updates are configured within the Computer Client Agent properties. The software update installation schedule can be modified from Configuration Manager Software Center on the client. You may also need to configure Group Policy settings on the client computer depending on your environment.

Computer Client Agent Settings

The properties for this client agent are found in various sections that provide configuration settings that affect the software update reminders and the customization for software update deployments on clients. In Figure 9.4, you see the relevant custom settings categories.

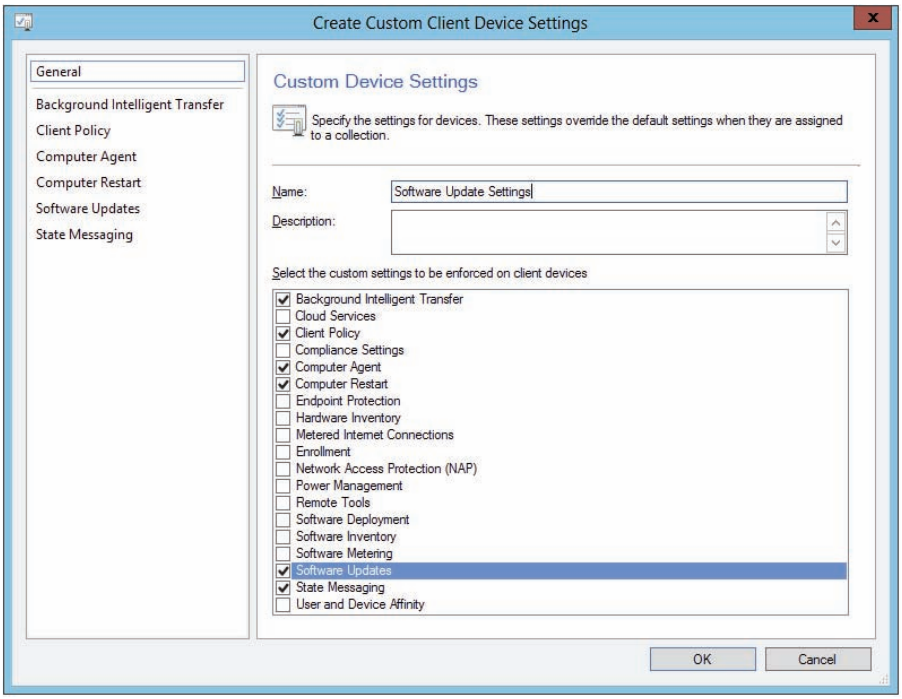


Figure 9.4
Computer client agent settings for software update deployment

Background Intelligent Transfer Section

The settings in this section specify if bandwidth throttling is configured for the site. These settings apply to Configuration Manager clients when they use BITS to download software update files from distribution points.

Client Policy Section

In the Client Policy section you can specify a polling interval, whether user policy should be allowed on clients, or whether to carry out user policy requests from Internet clients. The Policy Polling Interval (Minutes) setting controls how often clients retrieve the machine policy. This setting is relevant to software updates in that when new deployments are created, the machine policy is updated with the deployment information. Clients can take up to the policy polling interval to get those changes, depending on when they last got the policy. The default for this setting is 60 minutes.

Computer Agent Section

On this tab you can provide custom information about the updates that will appear on clients.

Reminder Settings The settings specify how often notifications are displayed on client computers when a deployment deadline is approaching for software updates. The reminder intervals can be configured for when the deadline is more than 24 hours away, when the deadline is less than 24 hours away, and when the deadline is less than an hour away.

Default Application Catalog Website Point You can configure the default application catalog website point so that the users can define their own working hours when going to the default application catalog website.

Organization Name This setting specifies the name of the organization authoring the software update install. By default this text box displays "IT Organization." The organization name appears in software update display notifications, the Available Software Updates dialog box, and the Restart Countdown dialog box on clients where software updates are deployed. Microsoft recommends that you customize this field with something related to your organization.

Computer Restart Section

These settings configure the start countdown timeframe and restart final notification when a software update is installed on client computers. By default, the initial countdown is 90 minutes, and a final notification is displayed when 15 minutes remain before the restart will occur.

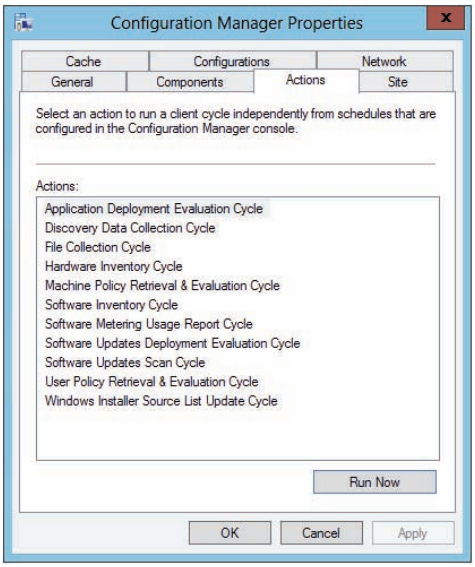
State Messaging Section

In the State Messaging section you can specify a reporting cycle for state messages. The State Message Reporting Cycle (Minutes) setting specifies how often clients send state messages to the management point. The software update client creates state messages for scan, software updates compliance, deployment evaluation, and deployment enforcement. The default setting for this is 15 minutes.

Client Configuration Manager Properties

The Configuration Manager Properties dialog box in the Control Panel of a Configuration Manager client provides software update actions and configuration settings. When you browse to the Actions tab, you can choose the following actions that are applicable for software updates, shown in Figure 9.5:

Figure 9.5
The Actions tab of the Configuration Manager client properties



Software Updates Deployment Evaluation Cycle When this action is started, active deployments will be evaluated.

Software Updates Scan Cycle This starts a software updates scan when run.

Software Settings Options

New in Configuration Manager 2012 is the Software Center, which is part of the Configuration Manager 2012 client. With the Software Center users can install or request software, but the users are also able to configure some settings that allow them to manage your software update deployment. A user can configure the Work Information and Computer Maintenance settings, shown previously in Figure 9.1:

Work Information You, as a user, can configure your business hours and business days. Once you define the hours and days, the software updates will be installed outside your work hours. Users can define business hours per hour from 12 a.m. until 11 p.m. and all hours in between, and they can choose the days by selecting a check box per day. You must reserve at least four hours each day for system maintenance tasks.

Computer Maintenance For software update installations users are able to choose to automatically install required software only outside of the specified business hours and restart

the computer if necessary or suspend Software Center activities when the computer is in a presentation mode.

Group Policy Settings

These settings in Group Policy are required for the Windows Update Agent on client computers to connect to WSUS on the software update point and successfully scan for software update compliance:

Specify Intranet Microsoft Update Service Location When the software update point is created for a site, clients receive a machine policy that provides the software update point server name and configures the Specify Intranet Microsoft Update Server Location local policy on the local computer. The WUA retrieves the server name set with Set The Intranet Update Service For Detecting Updates and then connects to that server when it scans for software update compliance. When a domain policy has been created for the Specify Intranet Microsoft Update Service Location setting, it will override local policy, and the WUA might connect to a server other than the software update point. If that happens, the client computer might scan for software update compliance based on different products, classes, and languages. Microsoft recommends that this domain policy *not* be configured for Configuration Manager clients; as mentioned earlier, you should disable the Group Policy settings when you already use a WSUS infrastructure in your environment.

Allow Signed Content From Intranet Microsoft Update Service Location Before the WUA on clients can scan for updates that were created and published with the System Center Updates Publisher, the Allow Signed Content From Intranet Microsoft Update Service Location Group Policy setting must be enabled. When the policy setting is enabled, the WUA will accept updates received through an Internet location if the updates are signed in the Trusted Publishers certificate store on the local computer.

Configure Automatic Updates The Automatic Updates feature allows clients to receive security updates and other important downloads. It is configured through the Configure Automatic Updates Group Policy setting of Control Panel on the local computer. When Automatic Updates is enabled, clients will receive update notifications (if you have notifications enabled) and download and install required updates. When Automatic Updates coexists with Configuration Manager 2012 R2 Software Updates, each might display notification icons and pop-up display notifications for the same update. Also, when a restart is required, each might display a Restart dialog box for the same reason.

Self-Update During a Configuration Manager client install, the Windows Update Agent is installed on a client computer if it is not already installed. When Automatic Updates is enabled, the WUA on each client automatically does a self-update when a newer version becomes available or when there are problems with the component. When Automatic Updates is not configured or is disabled, the WUA is still installed during Configuration Manager client installs. If the WUA install fails or becomes corrupt, or a new version of WUA is available, you must create a software distribution to update the agent on clients. If the WUA fails on a client, the scan for software update compliance also fails until it is fixed.

Role-Based Administration

For administering software update deployment, a special role is defined in the Role-Based Administration feature within Configuration Manager. An administrator who is added to the Software Update Manager role has the permissions delegated that are shown in Table 9.8.

TABLE 9.8: Permissions of the Software Update Manager role

OBJECT	PERMISSION
Alerts	Read, Modify, Delete, Create, Run Report, Modify Report
Boundary	Read
Boundary groups	Read
Client Agent Settings	Read
Collection	Read, Read Resource, Deploy Client Settings, Deploy Software Updates, Modify Client Status Alert
Deployment template	Read, Modify, Delete, Create
Distribution point	Read, Copy to Distribution Point
Distribution point group	Read, Copy to Distribution Point, Create Association to Collection
Query	Read
Site	Read
Software update groups	Read, Modify, Delete, Set Security Scope, Create
Software update package	Read, Modify, Delete, Set Security Scope, Create
Software updates	Read, Modify, Delete, Create, Move Objects, Modify Folder, Network Access, Run Report, Modify Report

Depending on whether the scope is limited or not, you can deploy the software updates to all Configuration Manager clients or a limited group of Configuration Manager clients. With Role-Based Administration, an administrator who is added to the Software Update Manager role sees only the objects that are related to the role.

System Center Updates Publisher

When planning to implement the current version of System Center Updates Publisher 2011, you need to be able to identify the following items.

Components of System Center Updates Publisher

System Center Updates Publisher 2011 consists of the following components:

Software Update Catalog Software Update Catalogs are used to import collections of related software updates into the System Center Updates Publisher repository.

Software Update The repository in the System Center Updates Publisher contains software updates that you can publish or export. You can import them via the update catalogs, or you can create them yourself.

Publications When publishing a software update to Configuration Manager 2012, you can publish either the full content of the software update or the metadata that describes the software update.

Rules When you publish software updates in System Center Updates Publisher, the applicability rules are used to check to see if the computer meets the prerequisites for the software update. It also checks to see if the software update is already installed on the computer.

Which Vendor Updates to Deploy

Currently three third-party custom software update partners publish catalogs that can be used via System Center Updates Publisher. You can import Software Update Catalogs from the following third-party hardware and software vendors: Adobe, Dell, and HP. Check this website for an up-to-date partner list:

```
http://technet.microsoft.com/en-us/systemcenter/cm/bb892875.aspx
```

The System Requirements

To be able to install System Center Updates Publisher, you need to be sure that the operating system complies with the following requirements:

- Windows Server Update Services 3.0 Service Pack 2 (WSUS 3.0 SP2)
- Windows Server Update Services 3.0 Service Pack 2 hotfix (KB2530678)
- Microsoft .NET Framework 4

Supported operating systems are these:

- Windows Vista
- Windows 7
- Windows 8.x
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Testing in an Isolated Lab

It is important to understand how software updates will work in your environment, and one way you can do that is to set up a test lab that is as close to your production environment as possible. This section describes a minimum setup of Configuration Manager to use while you are testing or evaluating the software update components and other deployments like applications and operating systems; always test your deployment in a test environment before deploying it in the production environment.

To start, you will need at least one computer for each operating system that you use in your environment. Also, you will need computers that have other crucial line-of-business applications running on them as well.

A single client is adequate for minimum test purposes, but if you want to have a representative sample of how software updates will work with all computers used in your enterprise, then you will need to have a representative of each client configuration in your environment. For example, if you are using Windows Server 2008 R2, Windows Server 2012 R2, Windows 7 SP1, and Windows 8.1 in your organization, then you should have at least one client with each of those operating systems on it for testing. If you can't get that many machines together, at least try to get one beefed-up computer with lots of RAM. That way, you can use Windows Server 2008/2012 Hyper-V or Windows 8 Hyper-V to set up virtual representations of the computers that you couldn't procure physically.

By doing this, you will become familiar with how the Software Updates components and the actual software update executables work with the operating systems on your network before you use Software Updates enterprise-wide. By using more than one operating system in your testing you will be able to do the following:

- Review the specific software updates that Microsoft has published for those operating systems.
- Start becoming familiar with software update management practices for each type of computer.
- Learn how software updates work with different operating systems in a controlled environment.
- Learn how to find information about specific software updates for a specific OS when you need it.

Requirements for Testing Software Update Points

When you test software updates, create the software update point site role as it would be in your production site. You will need to decide if a single software update point will be created or if there will be a software update point for connectivity from client computers on the Internet, and if the software update point will be set up with an NLB cluster. The deployment intelligence that you have gathered up to this point will be crucial to helping you plan your test environment.

Configuring Software Updates

Now that we have taken the time to look at the components of Software Updates and how they fit together, and you have taken that information with your deployment intelligence and put together a plan as to how you want to set up Software Updates in your environment, we can examine how to get everything working.

Before Software Updates data can be displayed in the Configuration Manager 2012 console and software updates can be deployed to clients, you must set up and configure the software update point, as well as the rest of the components of Software Updates.

Configuring the Software Updates Client Agent

The Software Updates Agent is enabled in Configuration Manager by default, but you still have to configure the other settings of this client agent to match your plans for using Software Updates in your environment.

To configure the Software Updates Agent, follow these steps:

1. In the Configuration Manager console, choose the Administration Workspace ➢ Overview ➢ Client Settings, and select the Default Client Agent Settings policy object.
2. Select the Home tab of the ribbon, and then click Properties.
3. Select Software Updates, and (as shown in Figure 9.6) configure the following settings:

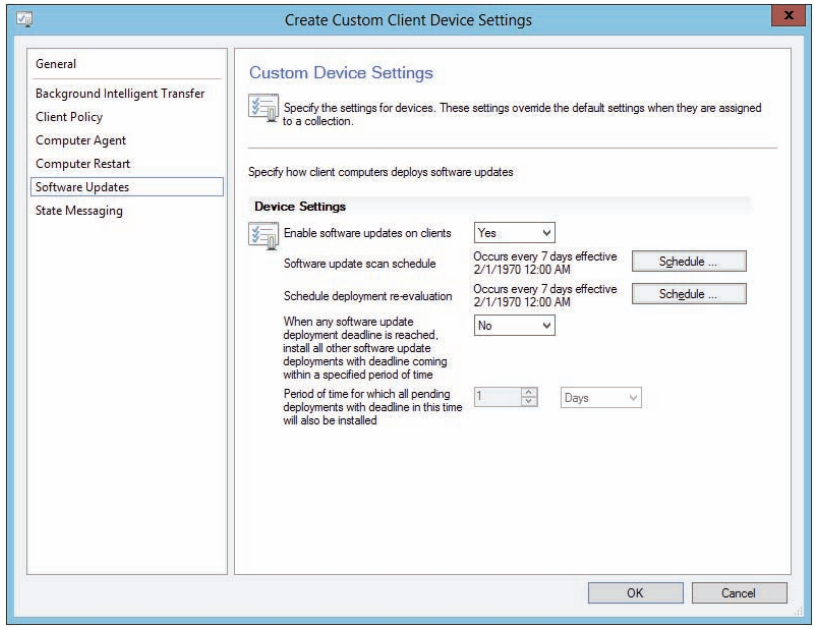


FIGURE 9.6
The default settings of the Software Updates Client Agent

Enable Software Updates On Clients This setting defines whether the Software Updates Agent is enabled for the site; this agent is installed and enabled on Configuration Manager clients by default. Make sure that this setting is enabled. If the client agent is disabled, the client agent components are put into a dormant state but not uninstalled, and existing deployment policies will be removed from clients as well. Re-enabling the client agent starts a policy request that the components on clients be enabled and the deployment metadata be downloaded. With Configuration Manager 2012 you can configure more than one client agent settings package. Chapter 6, "Client Installation," has more information about client agent settings.

Software Update Scan Schedule This setting specifies how often the client computer scans for software update compliance. By default, a simple schedule is configured to run the scan every 7 days, and the site database is updated with any changes since the last scan. The minimum value for the scan is 1 minute and the maximum value is 31 days. This setting can be configured only after a software update point site role has been installed on a site system in the site. When a custom schedule is configured, the actual start time on client computers is the start time plus a random amount of time up to 2 hours. This keeps all the clients from starting a scan and connecting to WSUS at the same time.

Schedule Deployment Re-evaluation You can configure how often the Software Updates Agent re-evaluates software updates for installation status. When software updates that have been installed are no longer found on client computers and are still required, they will be reinstalled. This re-evaluation schedule will need to be adjusted based on company policy for update compliance, whether users have the ability to uninstall updates, and similar considerations. You also have to consider that every re-evaluation cycle results in some network and client computer activity. The minimum value allowed for the deployment re-evaluation schedule is 1 minute and the maximum is one month. A simple schedule of every 7 days is set by default.

When Any Software Update Deployment Deadline Is Reached, Install All Other Software Update Deployments With Deadline Coming Within A Specified Period Of Time This setting indicates whether to enforce all mandatory software update deployments that have deadlines within a certain timeframe. When a deadline is reached for a mandatory software update deployment, an installation is started on the clients that have been targeted for the mandatory deployment. It also indicates whether to start the install for updates defined in other mandatory deployments that have a configured deadline within a specified timeframe. The benefits of this setting are that it expedites software update installs for mandatory updates and that it might increase security, decrease display notifications, and decrease system restarts on clients. This setting is disabled by default.

Period Of Time For Which All Pending Deployments With Deadline In This Time Will Also Be Installed This sets the timeframe for the software updates with a deadline to be installed if the deadline is coming within a specified period of time. The minimum value allowed is 1 to 23 hours, and the maximum is 1 to 365 days. By default, this setting is configured for 1 hour.

4. When you have finished setting things the way you want them, click OK to finish.

Installing Windows Server Update Services 3.0 Server

Windows Server Update Services 3.0 Server (WSUS) SP2 or later is required in order to use Software Updates in Configuration Manager 2012. Installing WSUS for use with Configuration Manager is different from a standard install of WSUS without the Configuration Manager infrastructure.

The WSUS installation procedure that we're going to use can be used for both the first software update point (the main software update point installed on the Central Administration Site) and all other software update points (those for any other primary Configuration Manager sites) or for installing WSUS on a remote server that is not a Configuration Manager site server. The decision to install WSUS on the same server as your site servers or on another remote server will depend on your server resources and your plans for the software update infrastructure.

Next, you have to go through a series of steps to make a software update point the active one for the Configuration Manager hierarchy. We will detail those steps later on in the chapter.

Depending on the version of your operating system, you need to either add the Windows Server Update Services role though the Server Manager of Windows Server 2008 R2 or Windows Server 2012 or make sure that you have downloaded the latest version of WSUS at the WSUS home page:

```
http://technet.microsoft.com/windowsserver/bb332157.aspx
```

Installing WSUS on Windows Server 2012 R2

To add the WSUS role to Windows Server 2012 R2, you need to perform the following steps:

1. Start the Windows Server 2012 R2 Server Manager from the Start screen.
2. In the Dashboard, click Manage and select Add Roles And Features to start the Add Roles and Features Wizard.
3. Click Next twice, select the server on which the WSUS role needs to be installed, and click Next again.
4. Select Windows Server Update Services, click Add Features, and click Next.
5. Click Next after reviewing the features that are automatically added. Click Next at the WSUS step to start the initial configuration of the WSUS role.
6. On the Roles Services step, select WSUS Services and Database and click Next.
7. On the Content step, disable the Store Updates In The Following Location option and click Next.
8. Supply the SQL Server And Instance Name (if necessary) and click Check Connection. Click Next.
9. On the Web Server Role (IIS) page, click Next.
10. On the Role Services page, click Next.
11. Specify an alternate source path if necessary; then click Install to begin the feature and roles installation.
12. After the installation is finished, start the Windows Server Update Services application from the Start screen to configure the WSUS role. Configure the database server where the WSUS database needs to be stored, and click Run to start the post-installation. Click Close when the post-installation is finished.

Installing WSUS on Windows Server 2008 R2

To add the WSUS role to Windows Server 2008 R2, perform the following steps:

1. Start the Windows Server 2008 R2 Server Manager from the Administrative Tools section of the console.
2. Click Roles and select Add Roles, and then click Next at the Before You Begin page.
3. Select Windows Server Update Services, and click Next.
4. Read the introduction to WSUS, and click Next.
5. Confirm the settings, and click Install.

   Once the download is finished, you will see the welcome screen of the WSUS 3.0 SP2 Setup Wizard.

6. Click Next.
7. Click the I Accept The Terms Of The License Agreement check box, and then click Next.

   If the Microsoft Report Viewer 2008 Redistributable is not installed, the Setup Wizard gives you a warning about it.
8. Click Next.
9. The next screen will ask you to choose if and where you want updates to be stored on the WSUS server, just click Next.
10. The next page lets you choose your database options:

    - If you are not installing WSUS on a Configuration Manager site, the default of Install Windows Internal Database On This Computer is probably your best option, because it installs Microsoft SQL Server 2005 Embedded Edition just for the purpose of managing WSUS. This will save you from having to purchase another full SQL Server license for WSUS and managing another instance of SQL as well.
    - If you are installing WSUS on a Configuration Manager Central Administration Site or a primary site server and it has the resources to handle it, then we recommend going ahead and using the instance of the SQL Server that is already installed. (If it doesn't have enough resources, you probably shouldn't be installing WSUS on this server anyway.) Having two versions of SQL installed on the same server could cause problems in the long run, and they would be competing for the same resources.

    Depending on what you choose, WSUS will either create the Windows Internal Database or test the connection to the existing SQL Server instance.
11. After that is done, click Next.
12. On the next page of the wizard, choose how to configure the WSUS website. Microsoft recommends that you choose to make a custom website if you are using WSUS as a software update point, even if the WSUS server is remote from the Configuration Manager site system. You should definitely use the custom site option if you are installing WSUS on a Configuration Manager site so that the install will not interfere with the other Configuration Manager components that use IIS. By default, the custom WSUS website uses HTTP port 8530 and HTTPS port 8531.
13. Click Next.
14. Review the settings, and click Next to install WSUS 3.0 SP2.
15. Click Finish and then Close after the installation.
16. The WSUS configuration wizard will start up after that, but you should close it, because Configuration Manager 2012 will take care of configuring all of the settings for WSUS.

Never Configure WSUS Using the WSUS Console

When you use WSUS in combination with the software update point role, you should never use the WSUS console to configure WSUS. Always use the Configuration Manager 2012 console to configure the software update point.

Installing the Downloaded WSUS Version

To install the downloaded version of WSUS, perform the following steps:

1. Double-click the WSUS install file that you downloaded, `WSUSSetup_30SP2_x86.exe` (or `WSUSSetup_30SP2_x64.exe` for the 64-bit version of Windows Server 2003), and you will see the opening page of the Windows Server Update Server 3.0 Setup Wizard.
2. Click Next, and then select Full Server Installation Including Administration Console and click Next again.
3. Click the I Accept The Terms Of The License Agreement check box, and then click Next.

   The next screen will ask you to choose if you want updates to be stored on the WSUS server and where you want to store them. You must accept the default and store a copy of these updates locally.
4. Choose where you want to keep these files, and then click Next.

   The next page lets you choose your database options.

   - If you are not installing WSUS on a Configuration Manager site, the default of Install Windows Internal Database On This Computer is probably your best option, because it installs Microsoft SQL Server 2005 Embedded Edition just for the purpose of managing WSUS. This will save you from having to purchase another full SQL Server license for WSUS and managing another instance of SQL as well.
   - If you are installing WSUS on a Configuration Manager primary site server and it has the resources to handle it, then we recommend going ahead and using the instance of the SQL Server that is already installed. (If it doesn't have the resources, you probably shouldn't be installing WSUS on this server anyway.) Having two versions of SQL installed on the same server could cause problems in the long run, and they would be competing for the same resources.

   Depending on what you choose, WSUS will either create the Windows Internal Database or test the connection to the existing SQL Server instance.
5. Once that is done, click Next.
6. The next page of the wizard, shown in Figure 9.6, lets you choose how to configure the WSUS website.

   Microsoft recommends that you choose to make a custom website if you are using WSUS as a software update point, even if the WSUS server is remote from the Configuration Manager site system. You should definitely use the custom site option if you are installing WSUS on a Configuration Manager site, so that the install will not interfere with the other Configuration Manager components that use IIS. By default, the custom WSUS website uses HTTP port 8530 and HTTPS 8531. Click Next.
7. Review the settings and click Next. When the wizard is done, click Finish. The WSUS configuration wizard will start up after that, but you should close it, because Configuration Manager will take care of configuring all of the settings for WSUS.

Installing the Windows Server Update Services 3.0 SP2 Administrative Console

The Windows Server Update Services 3.0 SP2 Administrative Console is required on the Configuration Manager 2012 site server, if WSUS is installed on a remote server, to allow it to communicate with WSUS so it can configure and synchronize software update points. The WSUS Administrative Console can be installed using the WSUS 3.0 Setup Wizard or installed silently from a command line.

To install the WSUS on a Configuration Manager site server, follow one of the procedures discussed in the sections that follow.

Installing the WSUS Administrative Console Using the Setup Wizard

Take the following steps to install the administrative console using the wizard:

1. Double-click the `WSUSSetup_30SP2_x86.exe` setup file that you downloaded earlier.
2. Click Next to get past the first page of the wizard, and then select Administrator Console Only. Click Next again.
3. Click I Accept The Terms Of The License Agreement, and click Next.
4. If you see the Required Components to Use Administration UI page, click Next.

   The Microsoft Report Viewer 2005 Redistributable will have to be installed, because it is required to open the WSUS console. It isn't needed when you are using WSUS with Configuration Manager, however.
5. When the wizard is done, click Finish.
6. To verify that the install completed, click Start ➢ All Programs ➢ Administrative Tools, and then choose Windows Server Update Services. To verify that connectivity, connect to the WSUS server that you are going to use with Configuration Manager.

Installing the WSUS 3.0 Administrative Console from the Command Prompt

Take the following steps to install the administrative console using the command line:

1. In the folder where you have already downloaded the WSUS installer file, open a command prompt.
2. In the command prompt window, type the following command:

   ```
   WSUS3Setupx86.exe /q CONSOLE_INSTALL=1
   ```

   The WSUS 3.0 SP2 administrative console will then install silently.
3. Verify the install as in step 6 of the previous procedure.

Setting Up the Software Update Point

There can be several Configuration Manager site systems with the software update point system role, but there can be only one site system server configured as the software update point that synchronizes with a synchronization source like Microsoft Update in a Configuration Manager

site. By default this is the first software update point you install in your environment. All other software update points are replicas of the first one you installed and use that one as the synchronization source.

When your Configuration Manager site is in HTTPS mode, you can have an Internet-based software update point assigned to a remote site system server that allows communication from only Internet-based client computers. Also, if the first software update point is on a Network Load Balancing cluster, there should be a software update point installed on every server that is in the NLB cluster. When you have a Central Administration Site in your Configuration Manager 2012 hierarchy, you first need to install and configure a software update point at one of the site servers in your Central Administration Site.

Setting Up the Software Update Point in the Central Administration Site

To set up a software update point in the Central Administration Site, you need to follow these steps.

1. In the Configuration Manager console, choose the Administration Workspace ➢ Overview ➢ Site Configuration ➢ Servers and Site System Roles.
2. Decide whether to create a new site system server or add the software update point role to an existing site system. Depending on which you choose, take the next step:
   - To create a new site system with a software update point, click Create Site System Server on the Home tab of the ribbon.
   - To add the software update point role to an existing server, do the following:
     a. Select the site server on which you want to install the software update point role.
     b. Choose Add Site System Roles in the Home tab of the ribbon.
3. Configure the server that is to be used for a site server, and click Next.

   See Figure 9.7 for the options for this choice.

   Specify An FQDN For This Site System For Use On The Internet You will have to configure this setting for a software update point when the site server is in secure mode or when it is in mixed mode and using Secure Sockets Layer (SSL).

   Internet FQDN You must configure this setting if you are setting up a software update point that accepts Internet-based client connections or for the active Internet-based software update point. It is only enabled when selecting the option Specify An FQDN For This Site System For Use On The Internet.

   Require The Site Server To Initiate Connections To This Site System You must use this setting when the remote software update point doesn't have access to the inboxes on the site server. This will let a site system from a different domain or forest place files that need to be transferred to the site server. The site server will connect to the remote site system and get the files periodically. The Internet-based software update point might need this setting to be enabled to work.

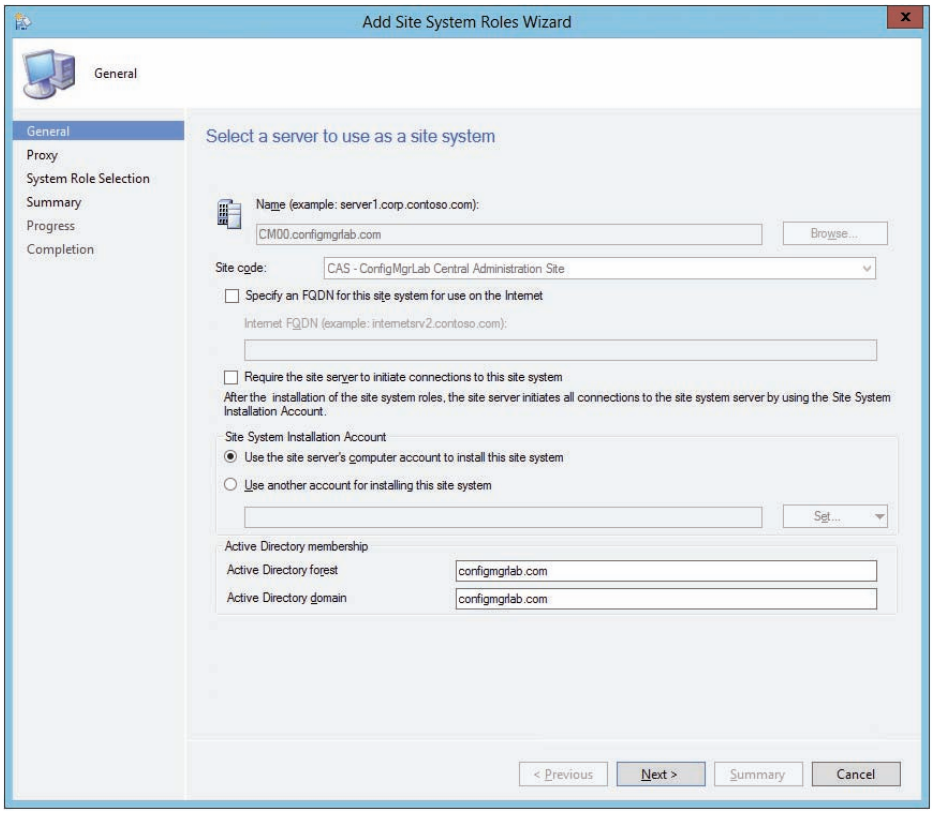


FIGURE 9.7 Configure the software update point settings.

Site System Installation Account Configure this setting when the computer account for the site server doesn't have access to the remote site system being set up as a software update point.

Active Directory Membership Configure the site system membership by supplying the forest and domain FQDNs.

4. If you need to go through a proxy server to get to the Internet, you will need to configure the proxy server and the possible credentials. If you have Internet access without a proxy server, just click Next.
5. Select software update point and click Next.
6. In the software update point page (see Figure 9.8), specify the port settings that are used by the WSUS you are connecting to. By default, the port settings for a WSUS custom website (the recommended settings) are HTTP port 8530 and HTTPS port 8531. If you installed WSUS on the default website, the ports are HTTP port 80 and HTTPS port 443. Click Next.

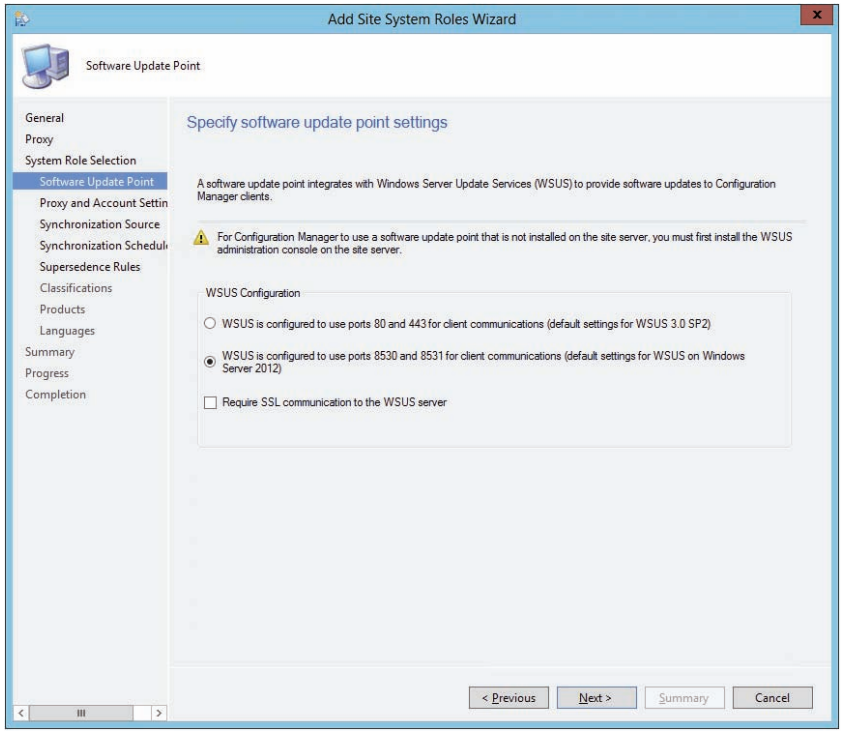


Figure 9.8 Configure the software update point port settings.

7. If your software update point is behind a proxy server on which you need to authenticate, you can enable the earlier configured proxy server access by enabling it by choosing Use A Proxy Server When Synchronizing Software Updates and/or Use A Proxy Server When Downloading Content By Using Automatic Deployment Rules. If authenticated access to the WSUS server is required, you can configure a WSUS Server Connection Account. Click Next when finished configuring the proxy and account settings.

8. Choose the synchronization source for the software update point by selecting one of the following options, and then click Next:

   Synchronize From Microsoft Update The software update point that is highest in the Configuration Manager hierarchy (usually the Central Administration Site) can use this setting. When an upstream software update point is in place, this option is not available.

   Synchronize From An Upstream Data Source Location (URL) If you do not want to synchronize directly with Microsoft Update but with another WSUS server, you can configure an upstream data source location. Normally it will be something like `https://wsusserver:8531` or `http://wsusserver:8530`.

   Do Not Synchronize From Microsoft Update Or Upstream Data Source Use this setting when the software update point can't connect to the upstream update server. This will usually be used by an active Internet-based software update point that doesn't have access to the software update point. The software update point on the CAS can't use

this setting. Synchronizing a software update point through importing and exporting updates is covered later in the chapter.

9. Configure the synchronization behavior of the software update role by selecting Enable Synchronization On A Schedule.

   This is disabled by default, and you can start a manual sync by running the Run Synchronization action in the Configuration Manager console. We recommend that you enable a schedule, because scheduled syncs perform full synchronizations, and manual syncs only do delta synchronizations of software updates.

10. Click Next after configuring the synchronization schedule.

11. Configure the supersedence behavior for updates that are about to expire, as shown in Figure 9.9. Choose one of the following:

    - Immediately Expire A Superseded Update
    - Do Not Expire A Superseded Software Update Until The Software Update Is Superseded For A Specified Period

12. Click Next.

13. Choose the update classifications that you want to deploy with software updates, and then click Next. You can change the classifications in a later stage.

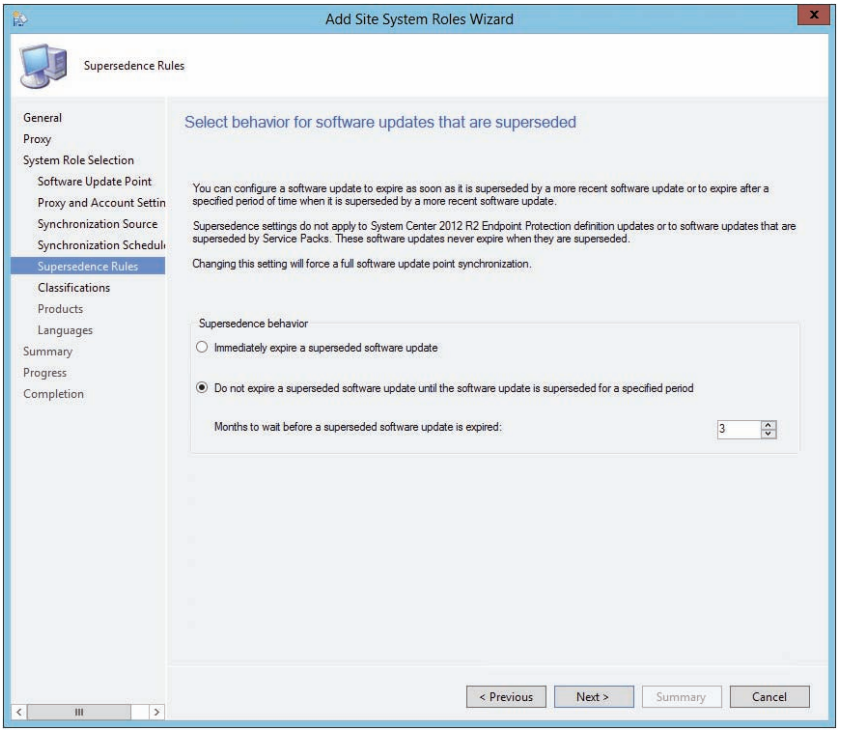


FIGURE 9.9 Configure behavior for software updates that are superseded.

14. Choose the products that you want to synchronize with software updates; you can change the products in a later stage. The number of products will change after the first synchronization with Microsoft Update has finished.
15. Select all the languages that you will be supporting with software updates, and then click Next.
16. Click Next again after reviewing the summary, and click Close after the installation is finished.

Setting Up the Software Update Point in a Primary Site That Is a Child of a CAS

To set up a software update point in a primary site that is a child of a Central Administration Site, follow these steps.

1. In the Configuration Manager console, choose the Administration Workspace ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Decide whether to create a new site system server or add the software update point role to an existing site system. Depending on which you choose, take the next step:
   - To create a new site system with software update point, click Create Site System Server on the Home tab of the ribbon.
   - To add the software update point role to an existing server, do the following:
     a. Select the site server on which you want to install the software update point role.
     b. Click Add Site System Roles on the Home tab of the ribbon.

   What you do next will depend on your site settings. By default, the computer account for the site server will connect to the site system computer (if you're installing on a separate site) and install the necessary components. If the computer account of the site server has access to the site system server and the Configuration Manager site is in HTTPS mode, the settings shown previously in Figure 9.7 are optional.
3. When the computer account does not have access to the site system server or when the site is in secure mode, you will have to configure the following settings on the New Site Role page:
   a. Specify An FQDN For This Site System For Use On The Internet

      By default, you will have to configure this setting for a software update point when the site server is in secure mode or when it is in mixed mode and using Secure Sockets Layer (SSL).

   b. Internet FQDN

      You must configure this setting if you are setting up a software update point that accepts Internet-based client connections or for the active Internet-based software update point.

c. Require The Site Server To Initiate Connections To This Site System

   This setting must be used when the remote software update point doesn't have access to the inboxes on the site server. This will let a site system from a different domain or forest add files that need to be transferred to the site server. The site server will connect to the remote site system and get the files every so often. The Internet-based software update point might need this setting to be enabled to work.

d. Site System Installation Account

   This setting is configured when the computer account for the site server doesn't have access to the remote site system being set up as a software update point.

e. Active Directory Membership

   Configure the site system membership by supplying the Forest and Domain FQDN.

4. After you have configured what you need, click Next.
5. If you need to go through a proxy server to get to the Internet, you will need to configure the proxy server and the possible credentials. If you have Internet access without a proxy server, just click Next.
6. Select software update point from the list of available site roles, and then click Next.
7. In the software update point page (see Figure 9.10), configure the port settings for a WSUS custom website (the recommended settings are HTTP port 8530 and HTTPS port 8531). If you installed WSUS on the default website, the ports are HTTP port 80 and HTTPS port 443.

   In the Client Connection Type section you need to configure what client connections are allowed for this software update point. Decide, depending on the purpose of the software update point, whether only intranet and/or Internet client connections are allowed.
8. If your software update point is behind a proxy server on which you need to authenticate, you can enable the earlier configured proxy server access by enabling it by choosing Use A Proxy Server When Synchronizing Software Updates and/or Use A Proxy Server When Downloading Content By Using Automatic Deployment Rules. If authenticated access to the WSUS server is required, you can configure a WSUS Server Connection Account. Click Next when finished configuring the proxy and account settings.
9. Review the summary, and click Next to start the installation of the software update point.
10. Click Close when the installation has finished.
11. After finishing the configuration of the software update point in the child primary site, you need to configure the supported languages for this software update point. In the Configuration Manager console, choose the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites, and select the child primary site in the hierarchy.
12. Choose Configure Site Components on the Settings section of the Home tab of the ribbon, and click software update point. In Figure 9.11 you see that it is recognized as a child site and that the upstream software update point is configured automatically. Select the Languages tab and configure the languages that you need to support. Be sure to configure languages that are available on the upstream software update point. Click OK when finished.

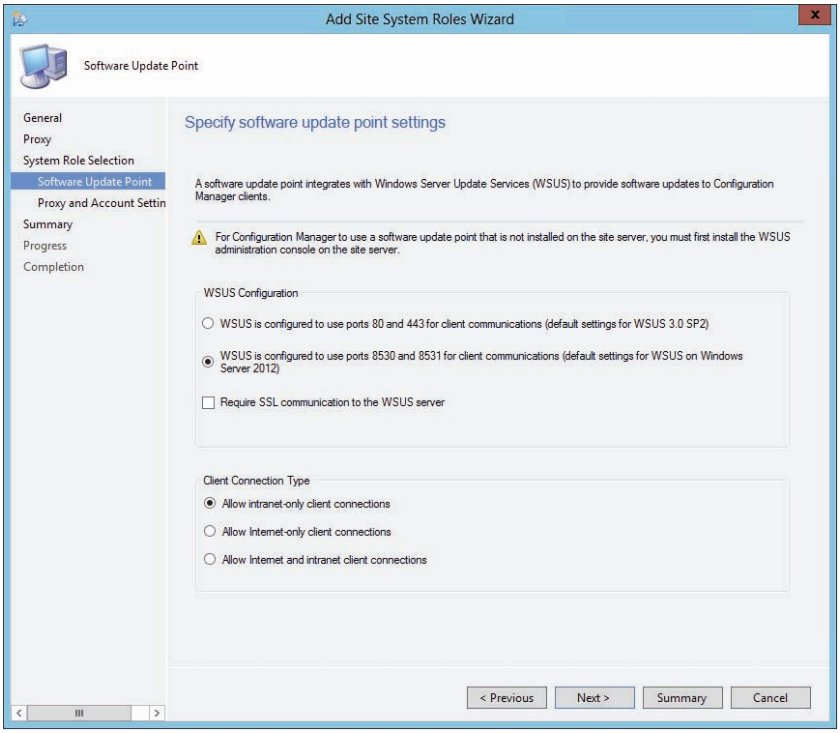


FIGURE 9.10
Specify software update point settings.

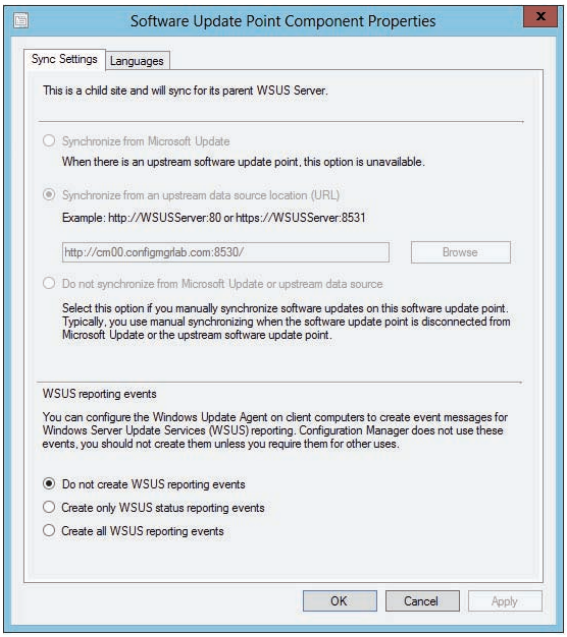


FIGURE 9.11
Software Updates Point Component Properties

Adding and Removing a Software Update Point with PowerShell

You are also able to add a software update point with the default Configuration Manager cmdlets in PowerShell. Adding a software update point on site server CM01 in the domain configmgrlab.com in primary site PS1 for only Intranet clients is done as follows:

```
Add-CMSoftwareUpdatePoint -SiteSystemServerName cm01.configmgrlab.com
-SiteCode ps1 -ClientConnectionType Intranet -WsusiisPort 8530
-WsusiissslPort 8531
```

Removing the same software update point can be done with the following command.

```
Remove-CMSoftwareUpdatePoint -SiteSystemServerName cm01.configmgrlab.com
-SiteCode ps1
```

Setting Up the Software Update Point in a Stand-alone Primary Site

A software update point can be installed in a hierarchy or at a stand-alone primary site. This section describes the installation steps of a software update point on a stand-alone primary site.

1. In the Configuration Manager console, choose the Administration workspace ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Decide whether to create a new site system server or add the software update point role to an existing site system. Depending on which you choose, take the next step:
   - To create a new site system with a software update point, click Create Site System Server on the Home tab of the ribbon.
   - To add the software update point role to an existing server, do the following:
     a. Select the site server on which you want to install the software update point role.
     b. Click Add Site System Role on the Home tab of the ribbon.

   What you do next will depend on your site settings. By default, the computer account for the site server will connect to the site system computer (if you're installing on a separate site) and install the necessary components. If the computer account of the site server has access to the site system server and the Configuration Manager site is in HTTPS mode, the settings shown previously in Figure 9.7 are optional.
3. When the computer account does not have access to the site system server or when the site is in secure mode, you will have to configure the following settings on the New Site Role page:
   a. Specify An FQDN For This Site System On The Intranet

      By default, you will have to configure this setting for a software update point when the site server is in secure mode or when it is in mixed mode and using SSL.
   b. Internet FQDN

You must configure this setting if you are setting up a software update point that accepts Internet-based client connections or for the active Internet-based software update point.

c. Require The Site Server To Initiate Connections To This Site System

   This setting must be used when the remote software update point doesn't have access to the inboxes on the site server. This will let a site system from a different domain or forest add files that need to be transferred to the site server. The site server will connect to the remote site system and get the files every so often. The Internet-based software update point might need this setting to be enabled to work.

d. Site System Installation Account

   This setting is configured when the computer account for the site server doesn't have access to the remote site system being set up as a software update point.

e. Active Directory Membership

   Configure the site system membership by supplying the forest and domain FQDNs.

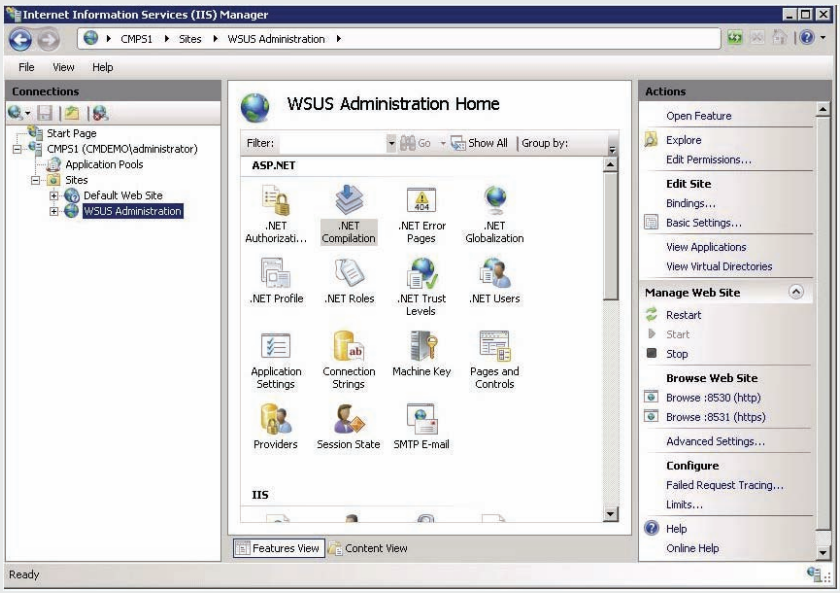
4. When you have configured what you need, click Next.
5. If you need to go through a proxy server to get to the Internet, you will need to configure the proxy server and the possible credentials. If you have Internet access without a proxy server, just click Next.
6. Select software update point from the list of available site roles, and then click Next.
7. In the software update point page (see Figure 9.10), specify the port settings that are used by the WSUS you are connecting to and which clients are allowed to connect to the software update point. Click Next after configuring the software update point server.

   By default, the port settings for a WSUS custom website (the recommended settings) are HTTP port 8530 and HTTPS port 8531. If you installed WSUS on the default website, the ports are HTTP port 80 and HTTPS port 443.

Finding the Ports Used by Windows Server Update Services

If someone else installed the WSUS server that is being used for a software update point, you may not know what ports were used during setup. If you input the wrong ports on this page of the wizard, the setup will fail. You can find the ports used by WSUS by following these steps:

1. Under Administrative Tools, click Internet Information Services (IIS) Manager.
2. Expand Sites, right-click the website that is being used for WSUS, and click Edit Bindings. A custom WSUS site is recommended, but the default website might have been used instead. The Port column will contain the number for the TCP port.
3. Look at the Browse Web Site list in the Actions section of the Management console; it will also contain the port list for the website.



8. If your software update point is behind a proxy server on which you need to authenticate, you can enable the earlier configured proxy server access by enabling it by choosing Use A Proxy Server When Synchronizing Software Updates and/or Use A Proxy Server When Downloading Content By Using Automatic Deployment Rules. If authenticated access to the WSUS server is required, you can configure a WSUS Server Connection Account. Click Next when finished configuring the proxy and account settings. Otherwise, just click Next. Choose the synchronization source for the software update point by selecting one of these options:

   Synchronize From Microsoft Update The software update point that is highest in the Configuration Manager hierarchy can synchronize from Microsoft Update; since you are installing it in a stand-alone primary site you may use this setting.

   Synchronize From An Upstream Data Source Location (URL) If you do not want to synchronize directly with Microsoft Update but with another WSUS server, you can configure an upstream data source location. Normally it will be something like `https://wsusserver:8531` or `http://wsusserver:8530`.

   Do Not Synchronize From Microsoft Update Or Upstream Data Source Use this setting when the software update point can't connect to the upstream update server. This will usually be used by an active Internet-based software update point that doesn't have access to the software update point. The software update point on the CAS can't use this setting. Synchronizing a software update point through importing and exporting updates is covered later in the chapter.

9. On that same page, accept the default of Do Not Create WSUS Reporting Events, and then click Next.
10. Always choose to synchronize software updates on a schedule by selecting Enable Synchronization On A Schedule.

    This is disabled by default; you can start a manual sync by running the Run Synchronization action in the Configuration Manager console. We recommend that you enable a schedule, because scheduled syncs perform full synchronizations and manual syncs only do delta synchronizations of software updates. Synchronizing a software update point manually is not a best practice.
11. Once you have made your choice, click Next.
12. Configure the supersedence behavior for updates that are about to expire, as shown previously in Figure 9.9. Choose one of the following:
    - Immediately Expire A Superseded Update
    - Do Not Expire A Superseded Software Update Until The Software Update Is Superseded For A Specified Period
13. Click Next.
14. Choose the update classifications that you want to deploy with software updates, and then click Next. You can change the update classifications in a later stage.
15. Choose the products that you want to synchronize, and then click Next. You can change the products in a later stage. The number of products will change after the first synchronization with Microsoft Update has finished.
16. Select all the languages that you will be supporting with software updates, and then click Next. You can change the supporting languages in a later stage.
17. Click Next again on the following page, and click Close.

Checking the Installation of the Software Update Point

After the installation of the software update point(s) it is a good idea to check some log files to be sure that the software update point(s) are installed correctly.

1. To monitor the install of the software update point, open the `SUPSetup.log` in the `<Configuration Manager Install Path>\Logs or %SMS_LOG_PATH%` folder.

   When the install has finished, you will see the text "Installation Was Successful."
2. Open the `WCM.log` in the same directory to verify that the connection to the WSUS server worked.

   When the connection to the WSUS server is made and the WSUS components are checked, you will see

   ```
   There are no unhealthy WSUS Server components on WSUS Server servername
   ```

   and

   ```
   Successfully checked database connection on WSUS server servername
   ```

   in the log file.

Configuring Software Updates Settings and Synchronization

Software updates in Configuration Manager 2012 must be synchronized with Microsoft Update or an upstream WSUS server before information on those updates will be available to view in the Configuration Manager console. Synchronization starts at the highest level in the hierarchy that has a software update point and either has a configured schedule or is started manually using the Run Synchronization action.

When synchronization is started on a configured schedule, all changes to the Software Updates metadata since the last scheduled sync are inserted into the site database. This will include metadata for new software updates or metadata that has been modified or deleted. When a sync is started manually, only new software updates metadata since the last sync is inserted into the database. The manual sync process is faster since it is not pulling as much Software Updates metadata. A manual sync action is available only on parent sites.

To manually sync the software update point, do the following:

1. In the Configuration Manager console, choose the Software Library workspace ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Select the Home tab of the ribbon and click Synchronize Software Updates. Click Yes to initiate a sitewide synchronization of software updates.

The synchronization process might take longer than an hour to finish, depending on several factors, including whether a synchronization has been run before and what languages, products, and update classifications have been configured to be synchronized. You can monitor the synchronization process by looking at the log file for WSUS Synchronization Manager, `wsyncmgr.log`. This is located by default at `%Program Files%/Microsoft Configuration Manager/Logs`.

When the synchronization is complete, you will see a 6702 status message from SMS_WSUS_SYNC_MANAGER.

New in Configuration Manager 2012 is that you also can monitor the synchronization in the Configuration Manager console.

To monitor the synchronization in the hierarchy do the following:

1. In the Configuration Manager console, choose the Monitoring workspace ➢ Overview ➢ software update point Synchronization Status.
2. Look at the synchronization status, the link state, and the catalog versions.

When the synchronization with Microsoft Update is complete (either from a schedule or started manually) at the highest site in the hierarchy, sync requests are sent to all child sites, and they in turn start synchronization with their configured upstream WSUS servers as soon as the request has finished processing.

The Software Updates metadata that is synced from Microsoft Update is based on the update classes, products, and languages that were selected when the software update point was first configured. A child site will synchronize whatever updates have been configured on its parent site.

Although all of the settings for update classes, products, and so on were configured at the setup of the software update point, you can still reconfigure these options if needed. To configure the update properties for software updates, follow these steps.

1. In the Configuration Manager console, choose the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites, and select the site that is the highest in the hierarchy.
2. Choose Configure Site Components on the Settings section of the Home tab of the ribbon, and click software update point.
3. To configure Update Classifications, click the Classifications tab, as shown in Figure 9.12.
4. To configure products that are being synced, click the Products tab, as shown in Figure 9.13.

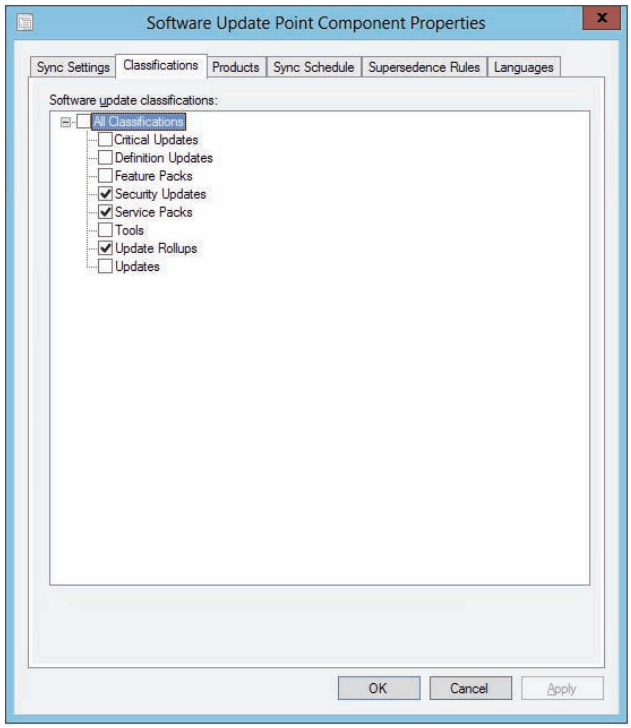


FIGURE 9.12
Software Update Point Component Properties: Classifications tab

5. To configure languages that are being synced, click the Languages tab, as shown in Figure 9.14.
6. To reconfigure the supersedence settings, click the Supersedence Rules tab, as shown in Figure 9.15.

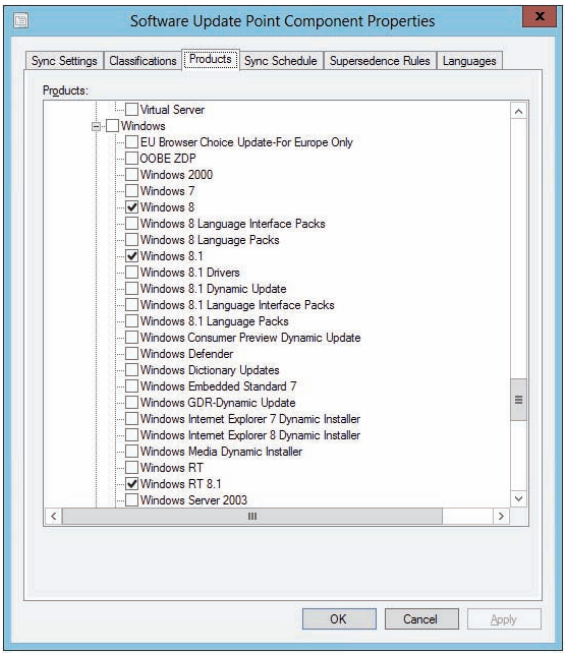


FIGURE 9.13
Software Update Point Component Properties: Products tab

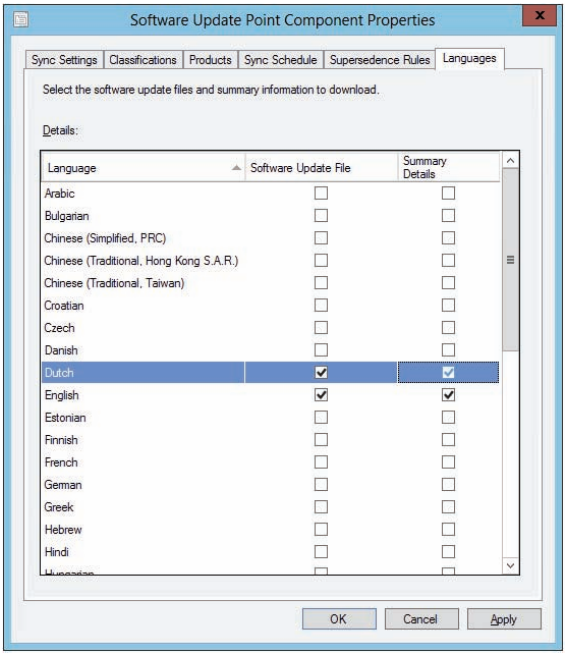
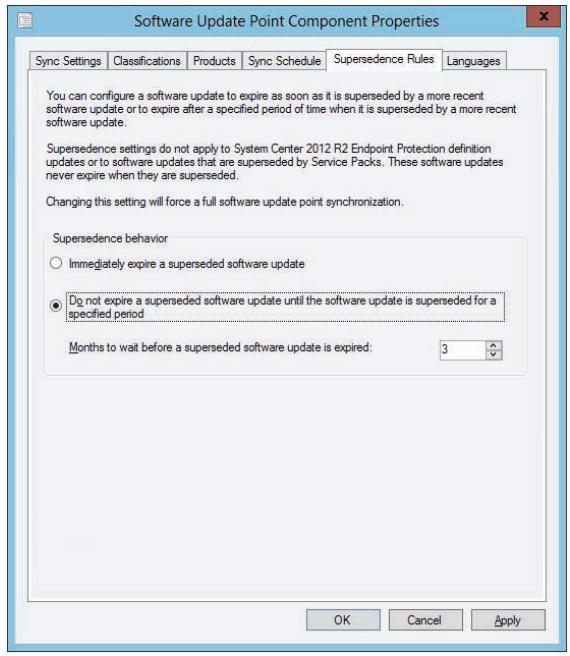


FIGURE 9.14
Software Update Point Component Properties: Languages tab

FIGURE 9.15
Software Update Point Component Properties: Supersedence Rules tab

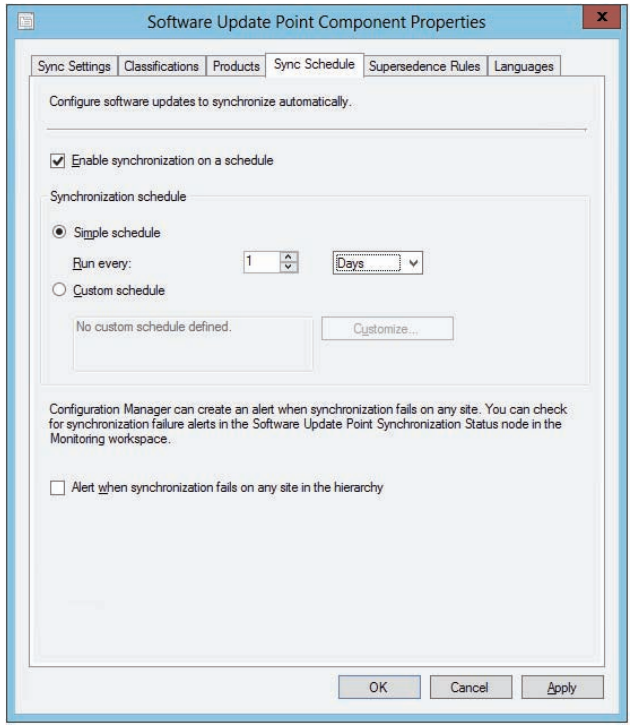


To configure the software updates synchronization schedule, follow these steps:

1. In the Configuration Manager console choose the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites, and select the site that is the highest in the hierarchy.
2. Choose Configure Site Components on the Settings section of the Home tab of the ribbon, and click software update point.
3. To configure the synchronization schedule, click the Sync Schedule tab, as shown in Figure 9.16.
4. To enable synchronization on a schedule, select Enable Synchronization On A Schedule, and set the schedule as you want it.
5. When you have finished, click OK to save the schedule.

   Unless you change the Start value in the custom schedule, synchronization will be started as soon as possible and will repeat based on the schedule that you configured.
6. If you want alerts to be reported in the Alerts node of the Configuration Manager 2012 console, enable the Alert When Synchronization Fails On Any Site In The Hierarchy option.

FIGURE 9.16
Software Update Point Component Properties: Sync Schedule tab



Synchronizing Updates with Export and Import

When a software update point is not configured or cannot synchronize with its upstream server in the Configuration Manager 2012 hierarchy, the export and import functions of the WSUSUtil tool can be used to synchronize Software Updates metadata manually. The user who performs the export/import must be a member of the local Administrators group on the WSUS server, and the tool must be run locally on the WSUS server itself.

The files found in the `WSUSContent` folder (by default located in `<WSUSInstallDrive>\WSUS\WSUSContent`) must also be copied from the upstream update server to the software update point so that locally stored updates and the license terms for the updates are available to the import server. This procedure can also be used for migrating the software update content from Configuration Manager 2007 to Configuration Manager 2012.

To export and import software updates from the export WSUS server to the import WSUS server, follow these steps:

1. Copy files from the export server to the import server:
   a. On the export server, go to the folder where software updates and the license terms for those software updates are stored. By default, this will be `<WSUSInstallDrive>\WSUS\WSUSContent`.
   b. Copy all of these files to the same folder on the import server.

2. Export metadata from the database of the export server:

   a. At a command prompt on the export WSUS server, go to the folder that contains `WSUSUtil.exe`. By default, this will be located at `%ProgramFiles%\Update Service\Tools`.

   b. Then enter the following:

      ```
      WSUSUTIL.exe export packagename logfile
      ```

      The name of *packagename* doesn't really matter, as long as it and the log file are unique in that folder. This command will export the Software Updates metadata into a file called `packagename.cab`.

   c. Move the export package that you just made to the folder that contains `WSUSUtil.exe` on the import WSUS server.

3. Import metadata to the database of the import server:

   a. At a command prompt on the WSUS server that you are importing the updates to, go to the folder that contains `WSUSUtil.exe`, which is `%Program Files%\Update Services\Tools`.

   b. Enter

      ```
      WSUSUTIL.exe import packagename logfile
      ```

      with *packagename* being the name of the export file that you exported in step 2.

      This will import all the metadata from the exporting server and create a log file that you can use to review the status.

Preparing Software Updates for Deployment

So far in this chapter, we have planned our implementation of Software Updates and set up and configured Software Updates, and now we are finally ready to deploy Software Updates to Configuration Manager 2012 clients. Well, nearly ready. We still need to find the updates to be deployed (using any of several methods), download them, and optionally create a software update group and/or an automatic deployment rule. These tasks can be done in the sequence shown here or independently of each other.

Before we get into that process, there are a few things you should keep in mind after you have set up all of the Software Updates components.

Give the process a little time to work. Don't expect to set up everything we have discussed so far and think you are going to be able to do a couple of clicks and deploy updates to your clients. You are going to have a little bit of lead time as updates are synced with Microsoft Update, the metadata is synced with the rest of the Configuration Manager hierarchy, and clients get requests for scans. Depending on the size of your hierarchy and the number and kind of clients you need to be scanned, this might take a while; after all, this is a process.

If you click the Software Updates node in the Configuration Manager console and don't see any results in your compliance summary, then your clients either haven't been scanned or they haven't sent their scan results. Until you see something in those reports, you don't have enough to work with to do any update deployments.

With that said, we can continue preparing for software update deployment.

Finding the Software Updates to Be Deployed

Before you can deploy any Software Updates to clients, you will need to figure out which ones you want or need to deploy to your clients. Configuration Manager provides several ways to do that, and each allows you to find clients that need the updates you want to focus on installed.

When you are looking for updates to deploy, avoid updates that show up in the Configuration Manager console with a yellow arrow icon. These are updates that have been superseded by another update that contains the same fixes. To avoid installing outdated components to your clients, do not include these updates in your deployments. They are no longer needed.

There are basically three methods to find needed software updates:

- Software Updates reports
- Software Updates search
- All Software Updates node

Using Software Updates Reports to Find Updates

You can gather compliance information on your clients by running reports under the Software Updates - A Compliance category, because they are designed specifically for this purpose.

To use web reports from the Configuration Manager console to find required updates, follow these steps.

1. In the Configuration Manager console, choose the Monitoring workspace ➢ Overview ➢ Reporting, expand Reports, and open the Software Updates - A Compliance folder.

   This will give you a list of all reports in the right pane of the console.

2. Find the report Compliance 4 - Updates By Vendor Month Year, select it, and click Run on the Home tab of the ribbon.

3. To get an idea of what update data you have collected already, do the following:

   a. Click Values for the collection All Systems.

   b. Click Values for the vendor Microsoft.

   c. Click Values for the update class Security Updates.

   d. Click Values for the current year (2013).

   e. Click View Report.

   You should see a report like the one shown in Figure 9.17.

   Any software updates that meet those criteria will be displayed in the report. The Required column gives the number of clients that require each software update in the list. The report also shows all of the updates that have been deployed by listing an asterisk (*) in the Approved column. To get more information about any of the updates, click the information link on the far right of the report (you may have to do some side scrolling to see it), and this will pull up the latest information from Microsoft on this update.

4. To get more details click the drill-down link in the first column of the report.

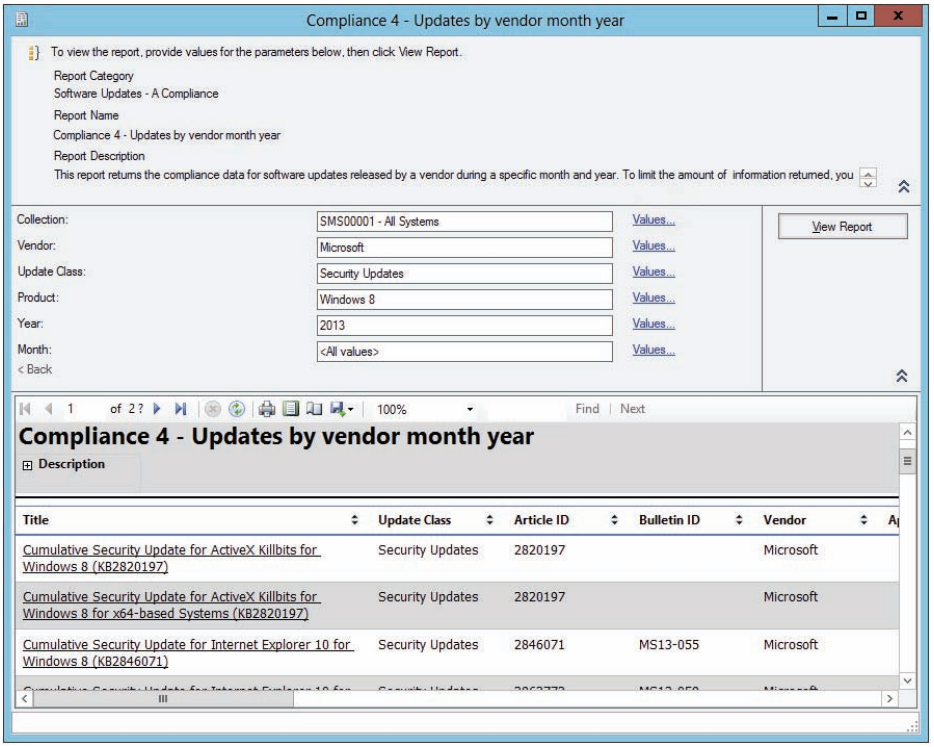


Figure 9.17
A sample compliance report with values entered for Collection ID, Vendor, Update Class, and Year

This will open the Compliance 6 - Specific Software Update States (Secondary) report, and you will see a count of computers for each compliance state for that particular update.

Using the Search Option in the Configuration Manager Console

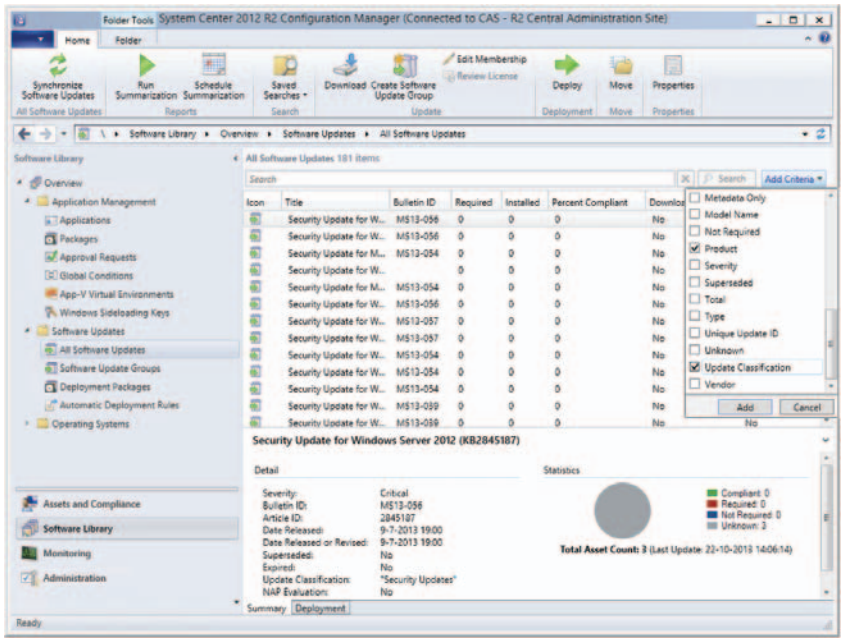
With the new Configuration Manager 2012 console you also have the ability to use a powerful search engine that comes with the console. Just under the ribbon, you will find the search option.

To use the search option to show software updates, follow these steps:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Click Add Criteria next to the Search button.

   You will then see the Criteria list box, as shown in Figure 9.18.
3. You want to search for all security updates for Windows Server 2012 R2. So first you scroll down and look for Update Classification (for security updates) and Product (for Windows Server 2012 R2).

FIGURE 9.18
Search criteria



4. Click Add to add the criteria to the search box.
5. To select the right product, click the link next to Product and select Windows Server 2012 R2.
6. To select the right update classification, click the link next to Update Classification and select Security Updates, as shown in Figure 9.19.
7. Click Search to activate the criteria.
8. To save the search for future use, you can click either Save Current Search or Save Current Search As in the Home tab of the ribbon of the Configuration Manager console.

You can find all the updates that need to be deployed to Windows Server 2012 R2 computers in this search by looking at the column labeled Required. You can sort by any column by clicking that column. From here you can download these updates, add them to an update group, or deploy them to client computers.

To manage and access saved searches, do the following:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Choose Saved Searches in the Search or Home tab of the ribbon of the Configuration Manager console, and click Manage Searches For Current Node.
3. Select the search you need, as shown in Figure 9.20, and click OK to make the search active. You can also rename or delete a saved search.

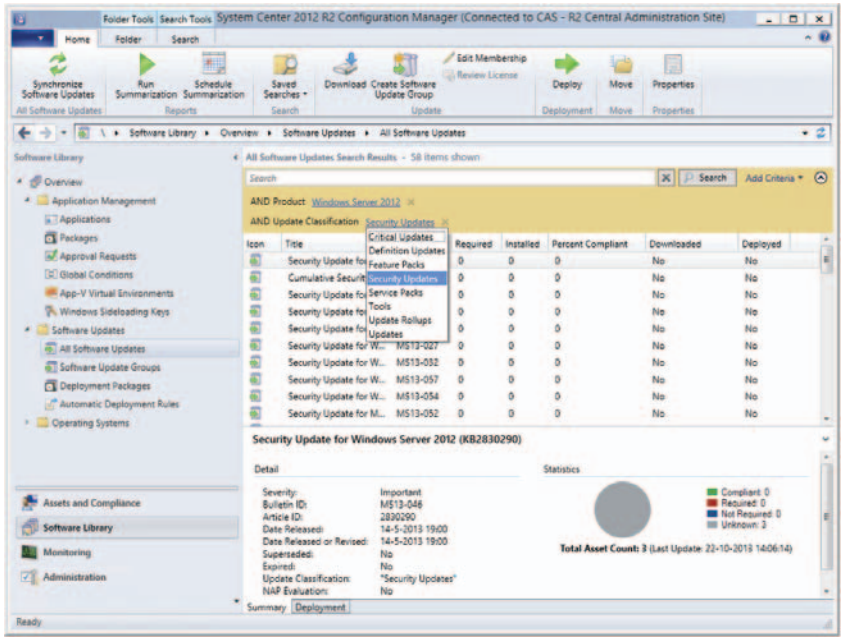


Figure 9.19
Adding search criteria to the search

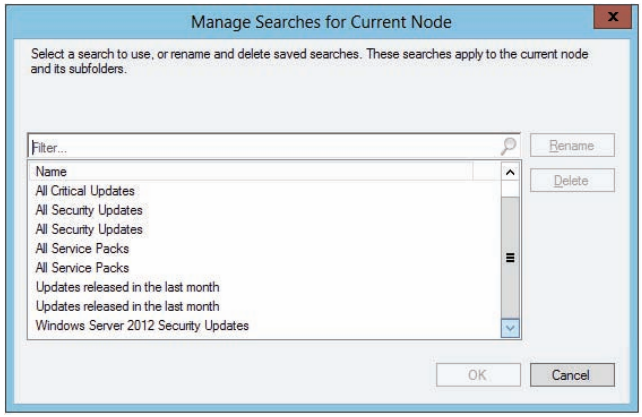


Figure 9.20
Selecting the search you need

Using the All Software Updates Node

When you browse in the Configuration Manager console to the All Software Updates node, you can select the software updates you want without using the search option.

To select the updates you want, do the following:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Browse to the update you want to deploy, or use the search option without the criteria to filter the updates.

Downloading Software Updates

As you saw in the last section, there are several ways to search for software updates that you want to download in Configuration Manager. The Download Updates Wizard allows you to download selected software updates to a deployment package prior to deploying updates to clients.

Software updates are downloaded from the Internet or from a shared folder on the network that the site server has access to and that can be added to new or existing deployment packages.

To download software updates to a deployment package, follow these steps:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Choose Saved Searches in the Search section of the Home tab of the ribbon of the Configuration Manager console, and click Manage Searches For Current Node.
3. Select the created Windows Server 2012 R2 Security Updates Search, and click OK.
4. Sort the updates in the list so that the updates required by the most clients are at the top by clicking the Required column twice.
5. Hold down the Shift key and select all the updates that have at least one client requiring that update.
6. Choose the Home tab of the ribbon, and click Download.

   This will start up the Download Software Updates Wizard, shown in Figure 9.21.

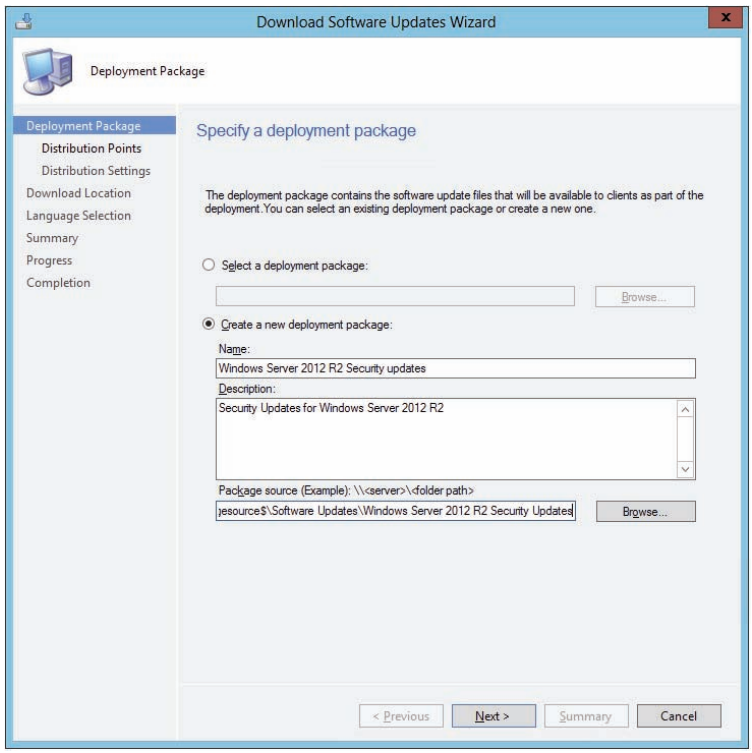


FIGURE 9.21 The Deployment Package page of the Download Software Updates Wizard

If you already have deployment packages created (as described later in the chapter), you can add these updates to one of them in the first field by selecting Select A Deployment Package. Then click Browse to open a dialog box that will allow you to select a package that is only for hosting software updates, and select one from the list. Otherwise, this option will be grayed out, as in our example.

7. The other option on this first page of the wizard is Create A New Deployment Package. There are three fields to fill out:

   Name The name of the deployment package. You should pick a unique name that describes the content and limit it to 50 characters or less.

   Description The description of the package contents up to 512 characters.

   Package Source The location of the software update source files. You should manually create this share before going any further. When the deployment is created, the source files are compressed and copied to the distribution points that are associated with the deployment package. This location must be entered as a network path (such as `\\server\sharename\path`), or you can click the Browse button to find the location on the network. This location should not be used by any other deployment or software distribution package.

8. After choosing the deployment package or supplying information for a new deployment package, click Next.

   The next step is the Distribution Points page. The Browse button allows you to select from the available distribution points or distribution point groups on your site that you want to use for this software update package. You can leave this blank for now, and the software update files will be downloaded to the source folder. However, the updates will not be available to deploy to clients until you add at least one distribution point.

9. After adding the distribution point(s), click Next to configure the distribution settings.

   In the Distribution Settings page, shown in Figure 9.22, the following options can be configured:

   Distribution Priority The distribution priority is used for the deployment package when it is sent to distribution points at child sites. Packages are sent in priority order of High, Medium, or Low. Packages with the same priority are sent in the order in which they are created. Unless there is a backlog, packages should process immediately no matter their priority. Medium is the default priority.

   Distribute The Content For This Package To Preferred Distribution Points When a client requests the content for this package and it is not available on any preferred distribution points for the client, specify if you want to distribute the content to the preferred distribution points.

   When you enabled content prestaging on your distribution points, because the scheduling synchronization and throttling of your bandwidth do not work for you, you also need to look at the following settings:

   Automatically Download Content When Packages Are Assigned To Distribution Points Use this option when smaller software update packages are used and scheduling and throttling settings provide enough control for the distribution of the content.

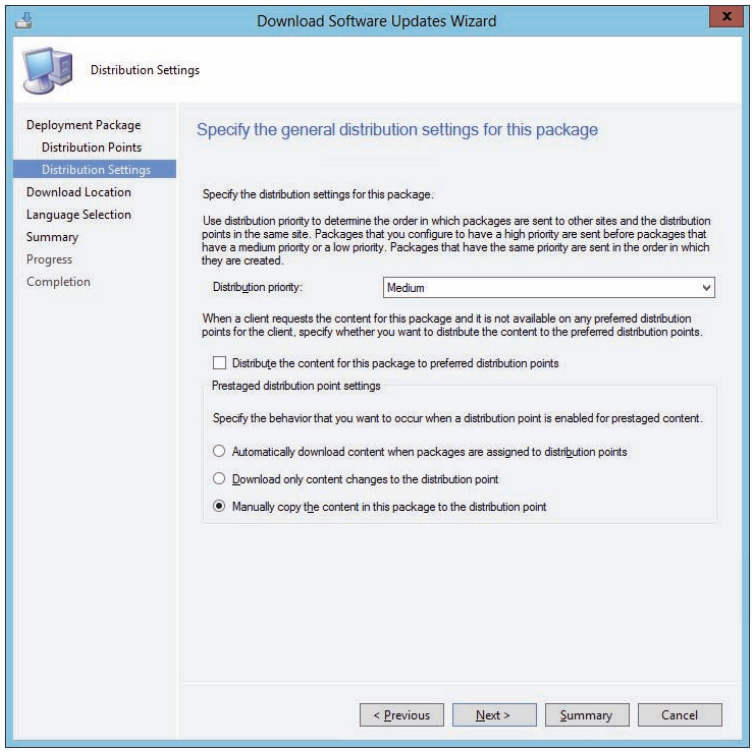


FIGURE 9.22 The Distribution Settings page of the Download Software Updates Wizard

Download Only Content Changes To The Distribution Point This option should be used when you have an initial package that is possibly large but you want to add future software updates to the content of this package.

Manually Copy The Content In This Package To The Distribution Point Use this option when you have large packages and you don't want to use the network for distribution of the content to the distribution point. You need to prestage the content on the distribution point.

10. Click Next when you've finished configuring the distribution settings.

Next is the Download Location page, with the following options:

Download Software Updates From The Internet This will download the updates from the location on the Internet that is defined in the software update definition. This is the default setting.

Download Software Updates From A Location On My Network The software updates are downloaded from a local directory or shared folder that you set in the box. Use this setting when the site server doesn't have Internet access. The software updates can be downloaded from any computer that does have Internet access and stored in a location on the local network that the site server has access to.

After configuring the download location, click Next. The Language Selection page shows the languages in which the software update files will be downloaded. By default, the languages that are configured for the software update point are selected. Adding a selection here does not add it to the software update point settings.

11. Click Next.
12. Review the settings and click Next; the updates will be downloaded.

When the wizard is done, the software updates will show up under Overview ➢ Software Updates ➢ Deployment Packages ➢ <*deployment package name*> in the Software Library workspace of the Configuration Manager console.

Creating a Software Update Group

As stated earlier in the chapter, a software update group in Configuration Manager contains a set of software updates. A software update group offers several benefits when deploying and monitoring software updates and is part of Microsoft's recommended Software Updates workflow.

Tracking the compliance state for the software updates in deployments is an important task for Configuration Manager administrators. When update groups are used, you can use the Compliance 1 - Overall Compliance report for the set of updates in the update group or the Compliance 3 - Update Group (Per Update) report to get a list of the updates in an update group and the overall compliance of each. This is a great reason to use the update groups as a part of your software update procedure.

To create a software update group, follow these steps:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates.
2. Choose Saved Searches in the Search area of the ribbon of the Configuration Manager console, and click More or use the Recent Searches option.
3. Select the created Windows Server 2012 Security Updates Search and click OK.
4. Sort the updates in the list so that the updates required by the most clients are at the top by clicking the Required column twice.
5. Hold down the Shift key and select all the updates that have at least one client requiring that update.
6. Click Create Software Update Group, and fill in the name and description of the software update group.
7. Click Create, and the software update group will be created.

Your new software update group will appear in the Software Update Group node under Software Updates in the Configuration Manager console.

Deploying Software Updates with the Deploy Software Updates Wizard

Now that all the setup and preparation tasks have been done, you are ready to run the deployment. Before deploying software updates, make sure you've considered things like whether the maintenance windows and client restart settings will work for the different clients

in your environment, how you are going to handle servers differently than workstations, and which deployments will be delegated.

To ensure the most successful software update deployments, utilize software update groups that fit the needs of your organization, and keep software updates organized so they are easier to keep track of and deploy.

The Deploy Software Updates Wizard in Configuration Manager allows you to create or modify software update deployments. You can select software updates that you want to deploy from several locations, as discussed earlier in this chapter, and you can start the deployment wizard in different ways as well.

To deploy software updates using the Deploy Software Updates Wizard, use the following steps:

1. In the Configuration Manager console, choose Software Library ➢ Overview ➢ Software Updates ➢ Software Update Groups.
2. Decide what updates you want to deploy.

   You can use any of the methods that were described in the "Finding the Software Updates to Be Deployed" section earlier in the chapter, or you can just select several updates from any of the Update Repository sections by Ctrl-clicking the updates that you want.
3. Start the Deploy Software Updates Wizard using either of the following methods:

   - Right-click some selected updates or a software update group, and then click Deploy.
   - Click Deploy on the Home tab of the ribbon of the Configuration Manager console after selecting some updates or a software update group.

   For this example, some updates that were not already downloaded were selected before clicking Deploy.

   The first page of the Deploy Software Updates Wizard is shown in Figure 9.23.
4. Configure the following options.

   Select Deployment Template If you have already saved a deployment template, you can select a saved deployment template. This template holds the most common settings.

   Deployment Name Give the deployment a name.

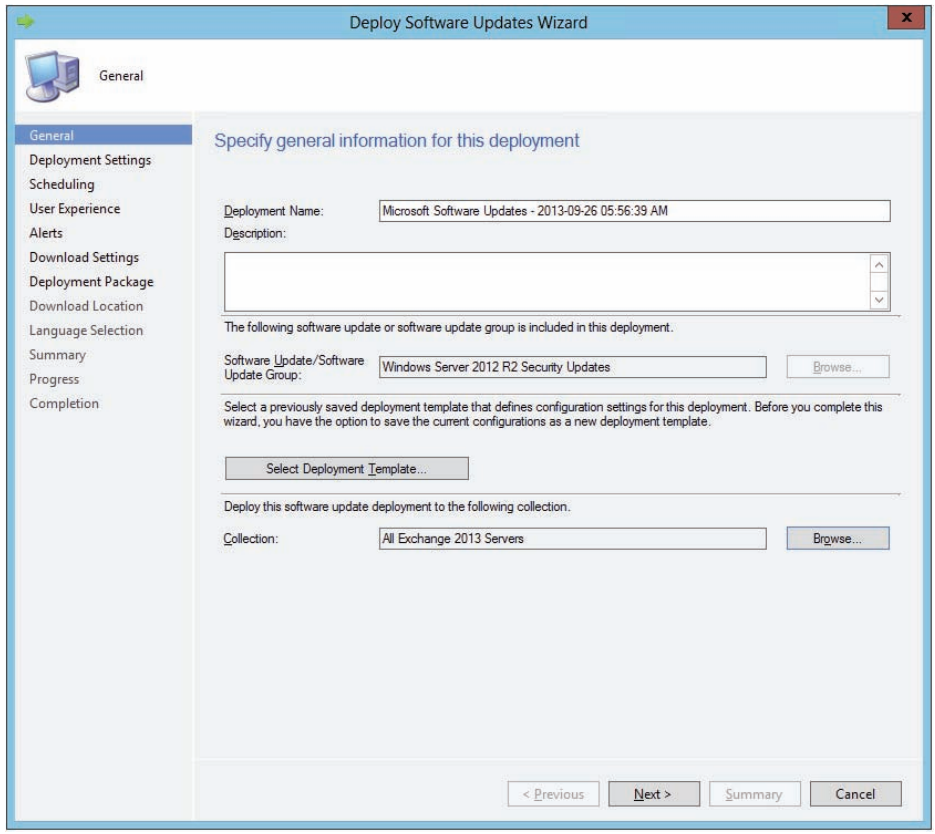
   Software Update/Software Update Group This option is active only when you select one or more updates instead of an update group.

   Collection Select the collection to which the deployment must deploy software updates.
5. Click Next.

   The next step in creating a deployment for deploying software updates is to configure the deployment settings. The configurable settings are as follows:

   Type Of Deployment Choose whether the deployment is available or required for installation. If the deployment is required, the installation of the software updates will start automatically, depending on the maintenance windows. If a deployment is available, the user is able to install the software updates. For software update deployments it is common practice to configure the deployment as required.

Figure 9.23
The General page



Use Wake-On-LAN To Wake Up Clients For Required Deployments Disabled by default, this option specifies whether at deadline Wake On LAN will be used to send wake-up packets to computers that require updates in the deployment. Be sure to configure the support of Wake On LAN in the Configuration Manager environment, your devices, and your network. See Chapter 4 for more information about configuring the support for sending wake-up packets.

Detail Level The detail level configures the state-message details that are returned by the clients for deployments. There are three levels that you can configure: All Messages, Only Success And Error Messages, or Only Error Messages.

6. Configure the settings and click Next.

The Scheduling page is next and is shown in Figure 9.24. This page has three sections:

Schedule Evaluation Select what the scheduled time must be based on: Client Local Time (the default) or UTC.

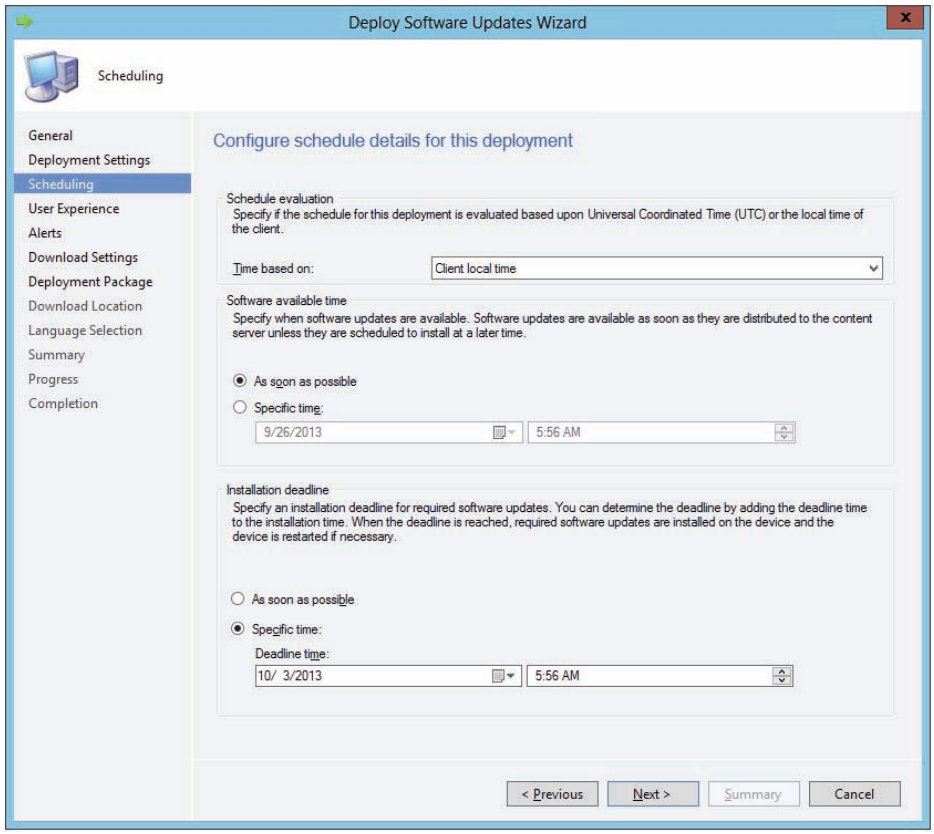


FIGURE 9.24
The Scheduling page

Software Available Time Select the date and time when software updates will be made available to clients: As Soon As Possible (the default) or Specific Time, which allows you to set a specific date and time when clients will be able to see the deployment.

Installation Deadline Specify whether the software updates should automatically install on clients at a configured deployment deadline:

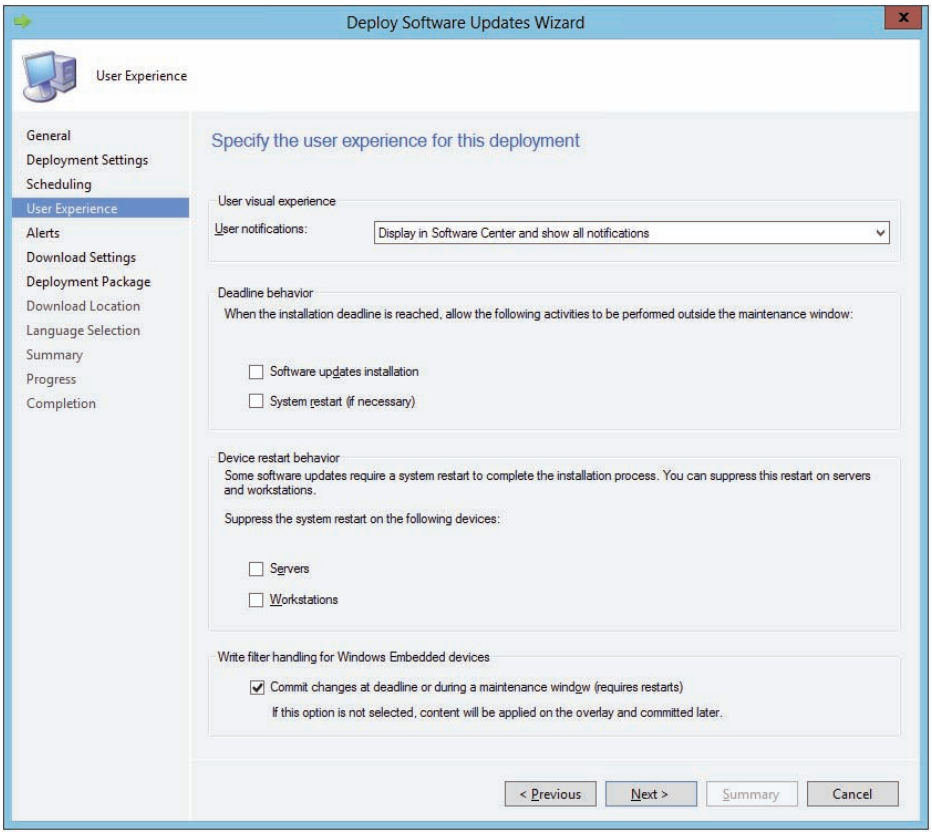
- As Soon As Possible
- Specific Time: Enabled by default, this allows you to set a date and time as a deadline for this deployment to be installed on clients.

7. Once you have made your choices on this page, click Next.

   The software updates will be available as soon as they have been distributed to the distribution points.

   The next step that you need to take is to configure the user experience; the options shown in Figure 9.25 can be configured.

FIGURE 9.25
The User Experience page



User Visual Experience You can set several options to configure the user experience when the software updates are deployed. You can hide software update installations and notifications from your users by selecting Hide In Software Center And All Notifications or choose Display In Software Center And Show All Notifications or Display In Software Center, And Only Show Notifications For Computer Restarts if you want notifications shown to your users.

Deadline Behavior When an installation deadline is reached, the installation can be performed outside the maintenance window, if you want. You can configure the actions by allowing an update installation and a system restart (if necessary) outside the maintenance window.

Device Restart Behavior Installing software updates on workstations or servers can initiate a system restart. With this setting you can suppress a system restart on workstations and servers.

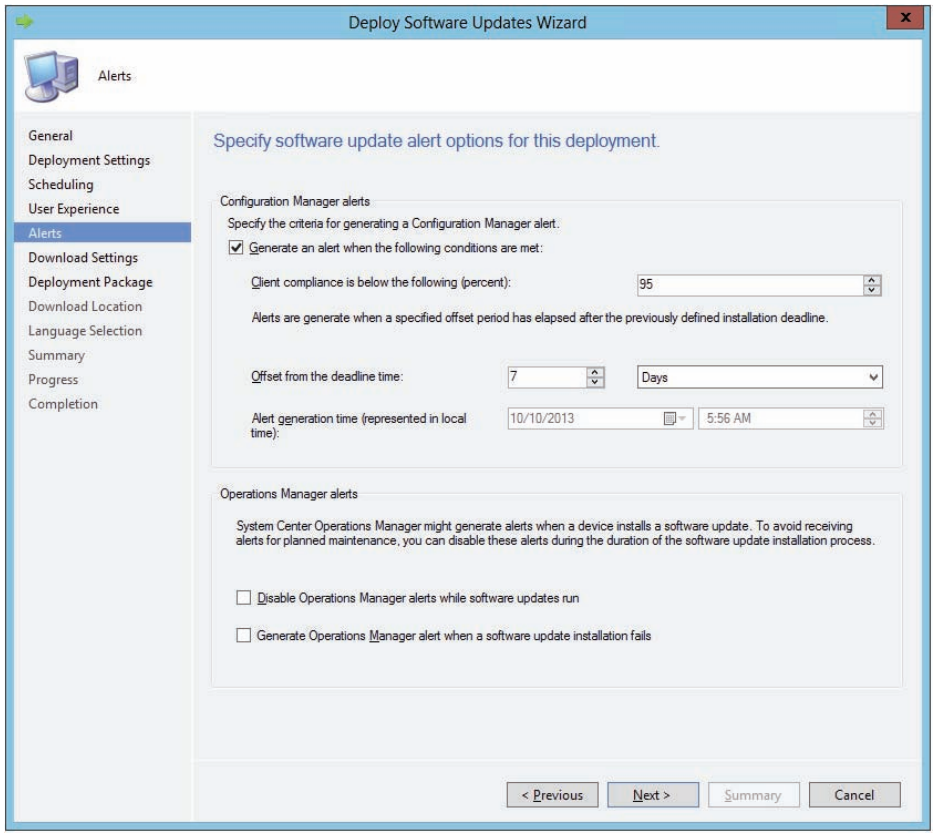
Write Filter Handling For Windows Embedded Devices When using Windows Embedded devices, write filters are in place to prevent the operating system from being changed by software or the users. The software updates agent in the Configuration Manager client is able to control the write filter so that the changes (software updates) are committed at the deadline or during maintenance windows. If this option is not selected, the software updates will be applied on the overlay and committed in a later stage.

8. Click Next when you have finished configuring the user experience.

   With the new alerting feature in Configuration Manager 2012, you can retrieve alerts in the Configuration Manager console and take actions when required.

9. Configure the options shown in Figure 9.26 for your organizational needs, and click Next.

FIGURE 9.26
The Alerts page



Configuration Manager Alerts This option is disabled by default, but it is recommended that you enable this option to get more control over the compliance level of your Configuration Manager clients. When you receive an alert that your compliance level is below a selected percentage, you can proactively take action to get the compliance at the right level.

Operations Manager Alerts Besides handling the alerting in the Configuration Manager console, you can retrieve your alerts by using Operations Manager. In this page you can disable the alerts for the duration of the software update installation.

10. Specify the download settings for your deployment. The page is divided into four sections:

    Download Settings For Slow Or Unreliable Network Define what to do if the Configuration Manager client is connected via a slow or unreliable network boundary. You can choose not to install the software updates or to download them from the distribution point and install them after downloading.

    Download Settings For Non-preferred Distribution Points Define what to do if the Configuration Manager client is connected via a network boundary with an unprotected distribution point. You can choose not to install the software updates or to download them from the unprotected distribution point and install them after downloading.

    Allow Clients To Share Content With Other Clients On The Same Subnet Select this option if you want to reduce the load on the WAN by allowing clients to download the Software Update content from other clients in the same subnet that already have downloaded and cached the content. This option uses Windows BranchCache.

    If Software Updates Are Not Available On Preferred Distribution Point Or Remote Distribution Point, Download Content From Microsoft Updates When the Configuration Manager client has already received a new list of updates that needs to be installed but the updates are not available on the preferred distribution point or a remote one, you can allow the client to download the software updates from Microsoft Update.

    Allow Clients On A Metered Internet Connection To Download Content After The Installation Deadline, Which Might Incur Additional Costs You can allow clients that are connected via a metered Internet connection (mobile data connection) to download their updates via this metered connection. Be aware if you enable this option that you might have extra costs for mobile data on your phone bill.

11. Click Next after configuring the download settings for the deployment.

    The next step is to select an existing deployment package to add the software update to or create a new software update package.

12. Click the first Browse button on the Deployment Package page and select one of the existing packages, or create a new deployment package. Then configure the settings that you need for creating a new deployment package:
Name Supply the name of the deployment package; be sure it is descriptive so you can identify the deployment package when you want to add other software updates to it.

    Description Supply the description of the deployment; be sure it is descriptive so you can identify the deployment package when you want to add other software updates to it.

    Package Source The package source is a UNC path to a location where the source of the deployment package will be stored. The UNC path must be available for the Configuration Manager site servers.

    Sending Priority The sending priority is used for the deployment package when it is sent to distribution points at child sites. Packages are sent in priority order from High, Medium, or Low. Packages with the same priority are sent in the order in which they were created. Unless there is a backlog, packages should process immediately no matter their priority. Medium is the default priority.

13. After configuring the deployment package, click Next, add the distribution point from which the deployment package must be available, and click Next again.

    The Download Location page appears with the following options:

    The Internet This will download the updates from the location on the Internet that is defined in the software update definition. This is the default setting.

    A Network Location The software updates are downloaded from a local directory or shared folder that you set here. Use this setting when the site server doesn't have Internet access. The software updates can be downloaded from any computer that does have Internet access and can be stored in a location on the local network that the site server has access to.

14. Configure where you want to retrieve the software updates from and click Next.

    The Language Selection page shows the languages in which the software update files will be downloaded. By default, the languages that are configured for the software update point are selected. Adding a selection here does not add it to the software update point settings.

15. Click Next.

16. On the Summary page shown in Figure 9.27, review the options you selected.

17. You can save all settings in a deployment template by clicking Save As Template.

    A dialog with all the settings will appear, as shown in Figure 9.28.

18. Name the deployment template and click Save.

19. After you have finished reviewing the Summary, click Next, and when the progress bar is done, click Close.

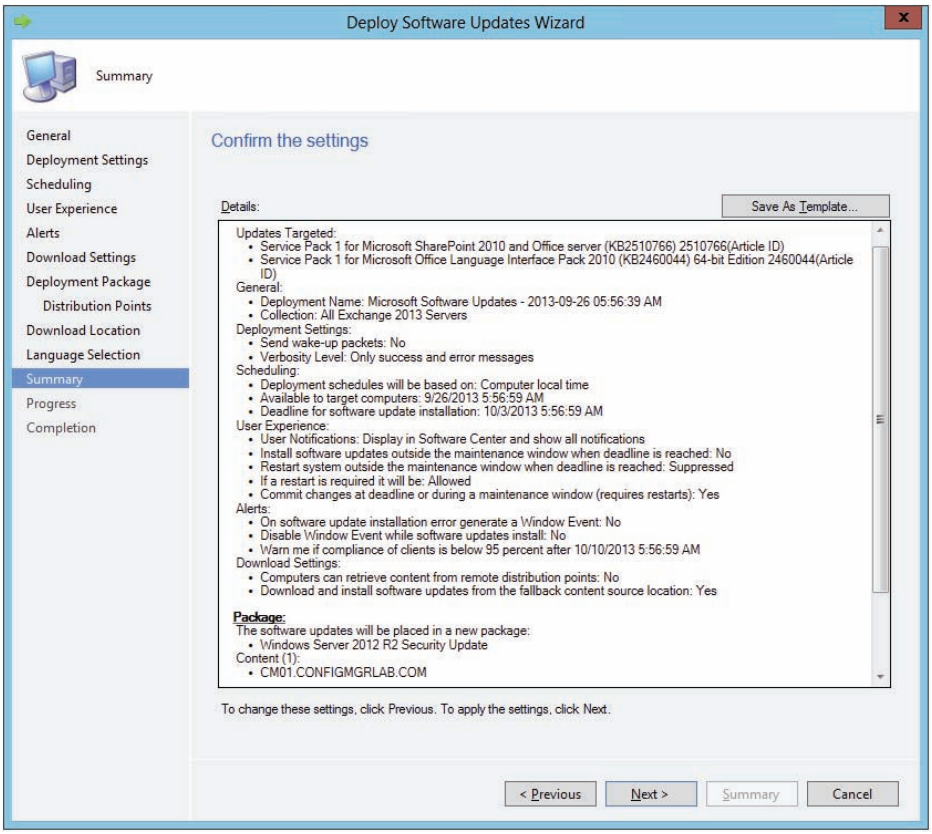


Figure 9.27
The Summary page

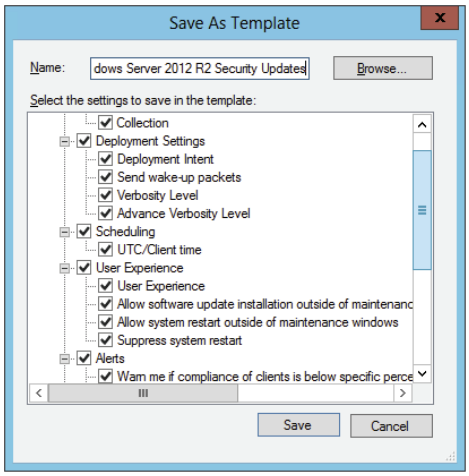


Figure 9.28
Name the deployment template

Using System Center Updates Publisher

With System Center Updates Publisher you can deploy software updates from third-party manufacturers. This section describes how to install and use System Center Updates Publisher.

Installing System Center Updates Publisher

After downloading the System Center Updates Publisher software and complying with the requirements, you need to install it. This section describes the installation process:

1. Go to the installation source of the System Center Updates Publisher and start `SystemCenterUpdatesPublisher.MSI`.
2. Click Next when the Setup Wizard starts.
3. If you are not using Windows Server 2012 and did not install the WSUS 3.0 hotfix (KB2530678), click the Install Microsoft Windows Server Update Services 3.0 SP2 Hotfix button, and download and install the hotfix, as shown in Figure 9.29.

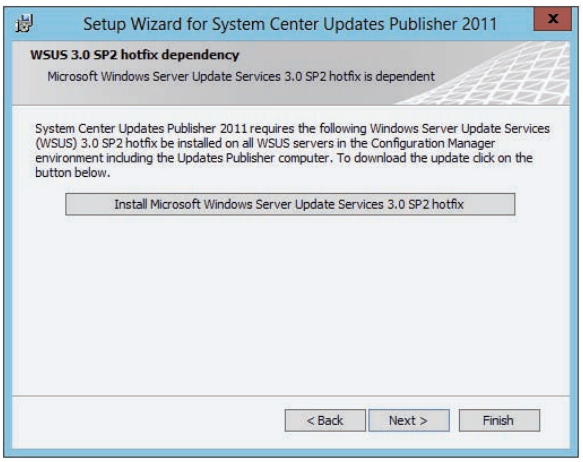


FIGURE 9.29
Download the WSUS 3.0 SP2 hotfix

4. Click Next.
5. Select I Accept The License Agreement, and click Next.
6. Define the installation location, and click Next twice.
7. Click Finish when the installation is complete.

Configuring System Center Updates Publisher

Next, you must configure System Center Updates Publisher so that it's able to publish software updates to the WSUS 3.0 SP2 server:

1. Start the System Center Updates Publisher 2011 console from the Start menu within Windows.

   The console will start, as shown in Figure 9.30.

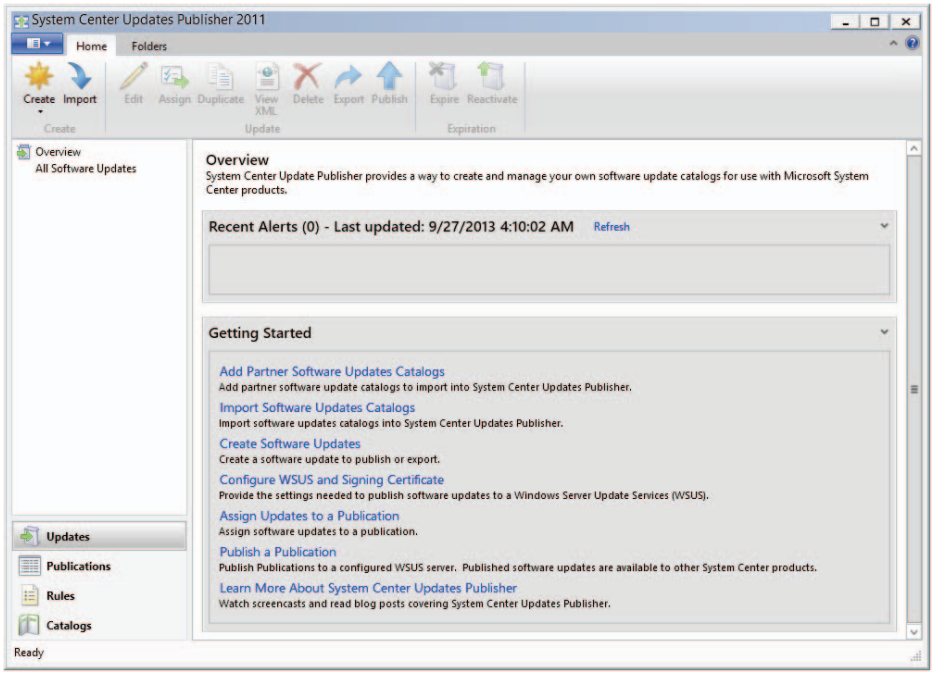


FIGURE 9.30
The System Center Updates Publisher 2011 console

2. Click Configure WSUS And Signing Certificate to configure the System Center Updates Publisher options, shown in the right column of the console.

   Update Server Configure an update server by choosing Enable Publishing To An Update Server. Whether your WSUS server is installed locally or remotely, select the appropriate option to configure the WSUS server, as shown in Figure 9.31. Supply a signing certificate or create a self-signed certificate. Be sure that your computers also trust the certificates that are used to sign the software updates.

   ConfigMgr Server Configure the connection with your Configuration Manager 2012 server and test the connection. If you have installed System Center Updates Publisher on a remote server, also configure the thresholds.

   Trusted Publishers If you accept the certificates of the publishers while importing catalogs, you can remove or view them here.

   Proxy Settings Configure the proxy settings if you need to use a proxy to connect to the Internet.

   Advanced If you are signing updates, you need to choose the Enable Add Timestamp When Signing Updates option. You can also configure security and local source publishing settings.

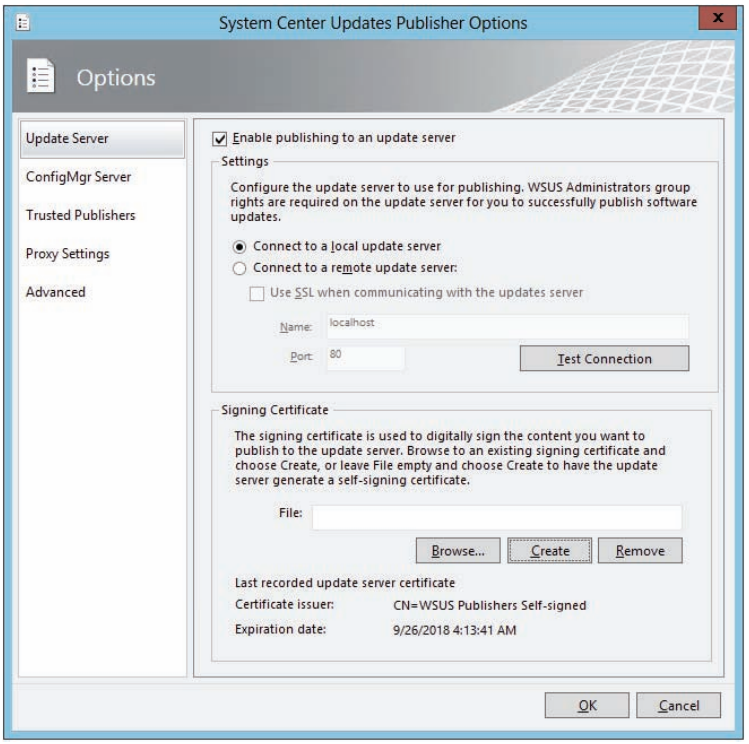


FIGURE 9.31
Enable publishing to an update server

Using System Center Updates Publisher

When using System Center Updates Publisher you need to go through the following steps:

1. Add partner software updates catalogs.
2. Import updates.
3. Create rules.
4. Publish updates.

ADDING PARTNER SOFTWARE UPDATES CATALOGS

After configuring System Center Updates Publisher, the next step is to add partner software updates catalogs.

1. Start the System Center Updates Publisher 2011 console from the Start menu within Windows.
2. Click Add Partner Software Updates Catalogs.

3. Select the partner catalogs you want to use, and add them to the Selected Partner Catalogs list, as shown in Figure 9.32.
4. Click OK.

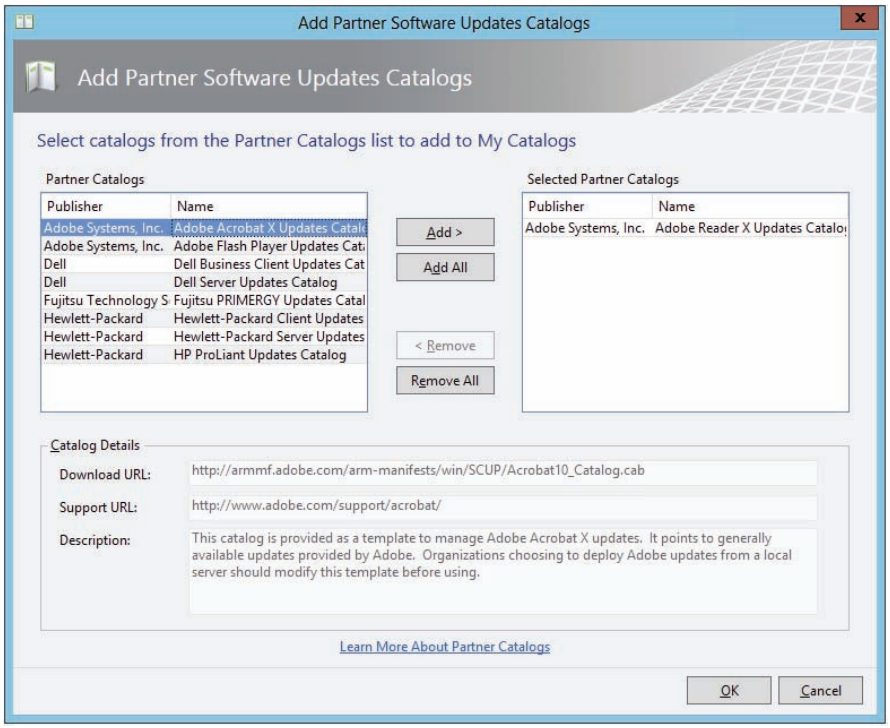


Figure 9.32
Adding partner catalogs

Importing Updates

The next step after adding the partner software updates catalogs is importing the updates to System Center Updates Publisher.

1. Start the System Center Updates Publisher 2011 console from the Start menu within Windows.
2. Click Import Software Updates Catalogs, select the update catalogs, as shown in Figure 9.33, and click Next.
3. Confirm the settings and click Next.

   While downloading the catalogs you will see a security warning, as shown in Figure 9.34.
4. Review the certificate, select Always Accept Content From "*Publisher*," and click Accept.
5. Click Close once the import is ready.

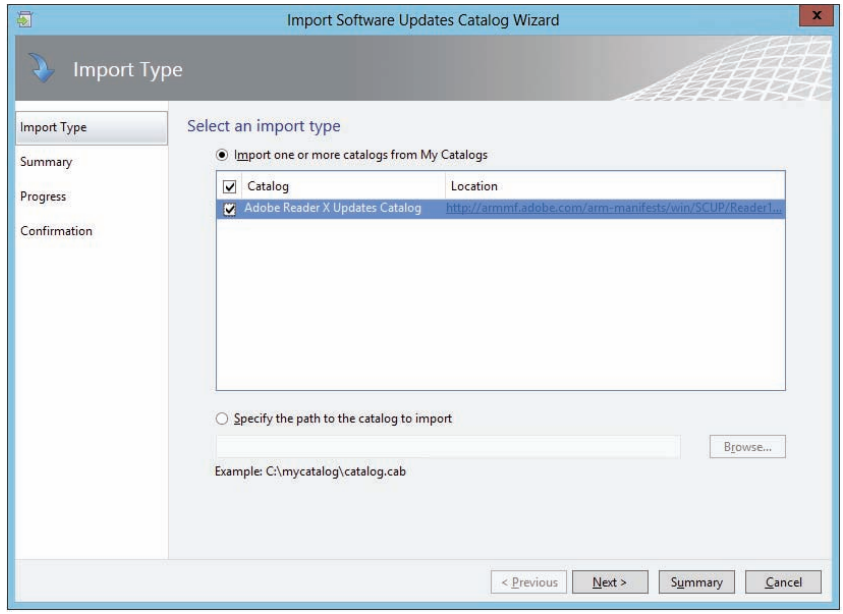


FIGURE 9.33
Importing the update catalogs



FIGURE 9.34
Accept the catalogs

CREATING RULES

With applicability rules you can define which updates can be deployed on what kind of operating system.

1. Start the System Center Updates Publisher 2011 console from the Start menu within Windows.
2. Click Create on the Home tab of the ribbon in the Rules workspace.
3. Supply a rule name, and click the yellow star icon to add a rule.

   You can configure different kinds of rules based on file, registry, system, or Windows Installer properties.

4. Configure the rule like the example for Windows 8 shown in Figure 9.35.

   You can add AND or OR operators to the statement, as shown in Figure 9.36, and click OK.

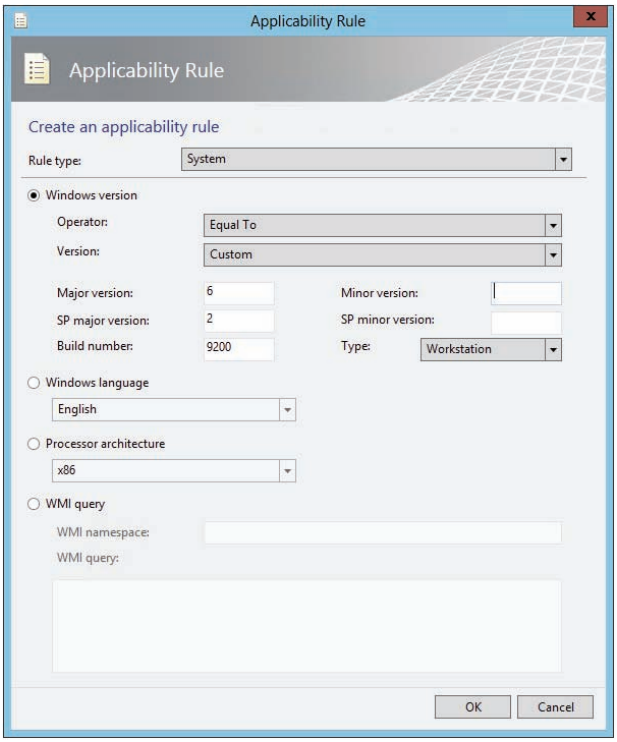


FIGURE 9.35
Configure the rule like you want.

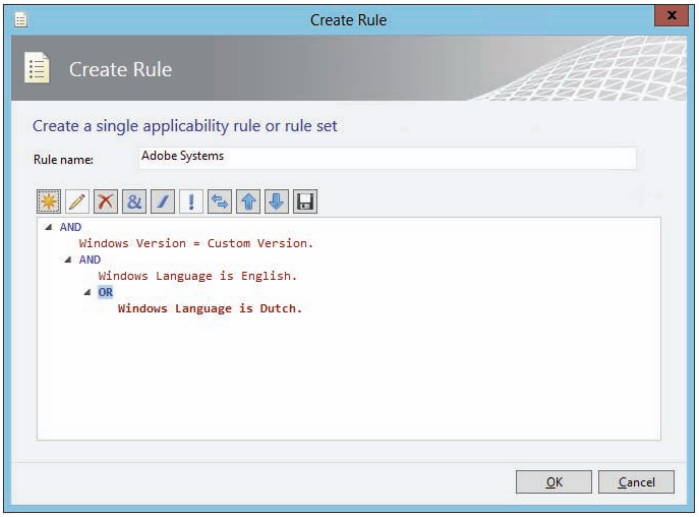


FIGURE 9.36
Combined rule statement

Publishing Updates

After assigning the update catalogs, importing them, and creating rules, the next step is to publish the updates to Configuration Manager 2012 so that you can deploy the updates.

1. Start the System Center Updates Publisher 2011 console from the Start menu within Windows.
2. Choose the Updates workspace, and select the updates you want to publish.
3. Click Publish on the Home tab of the ribbon.
4. Select the publish option you want, as shown in Figure 9.37.

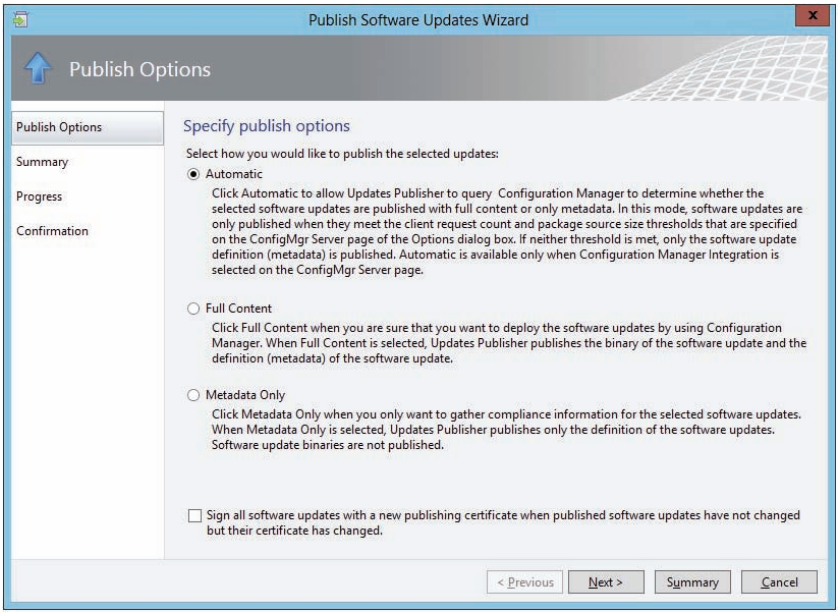


Figure 9.37 Select the appropriate publish option.

Automatic This option lets Configuration Manager determine whether the selected software updates are published with full content or metadata only. When you select this option, software updates are published only when they meet the client request count and package source size thresholds that are configured at the Configuration Manager Server section while configuring the connection. If the thresholds are not met, only metadata will be published.

Full Content When this option is selected, Updates Publisher publishes the binary and the metadata of the software update.

Metadata Only When this option is selected, Updates Publisher publishes the metadata of the software update.

5. Select Sign All Software Updates With A New Publishing Certificate When Published Software Updates Have Not Changed But Their Certificate Has Changed, and click Next.
6. Confirm the settings and click Next.
7. After the updates are published, as shown in Figure 9.38, click Close.

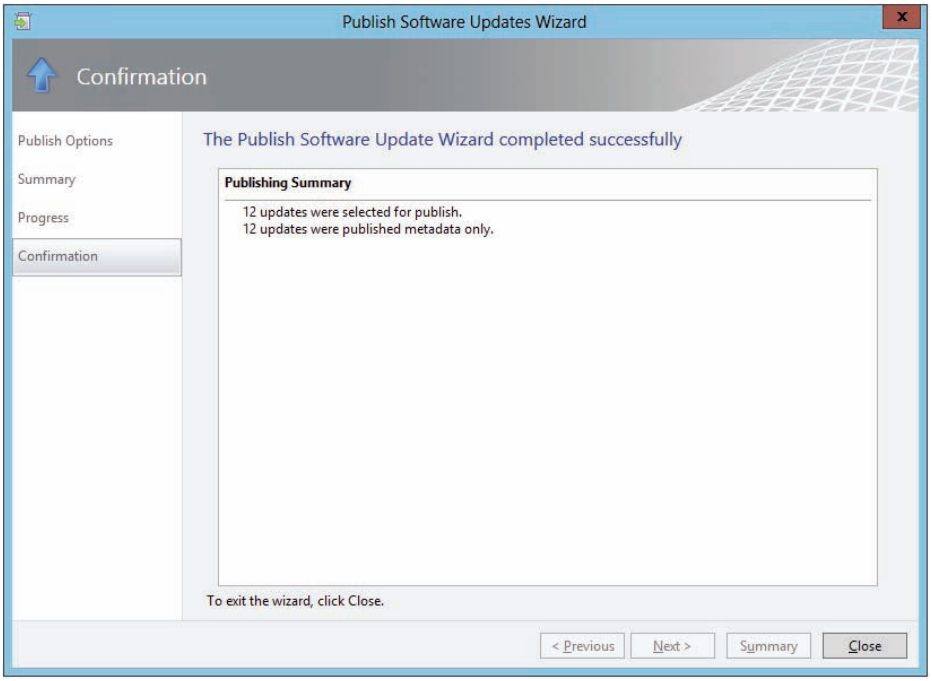


FIGURE 9.38
Confirmation page of the Publish Software Updates Wizard

Third-Party Updates in Configuration Manager

To be able to deploy the third-party software updates with Configuration Manager, you need to configure the software update point component to also synchronize the software updates:

1. In the Configuration Manager console choose the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites and select the highest site in the hierarchy.
2. Choose Configure Site Components on the Settings section of the Home tab of the ribbon, and click software update point.
3. To configure the third-party software updates, click the Products tab, as shown in Figure 9.39. If the third-party updates are not yet available, manually synchronize the software updates.
4. After you synchronize the software updates, the third-party updates will become available in Configuration Manager, as shown in Figure 9.40.

FIGURE 9.39
Select the third-party updates.

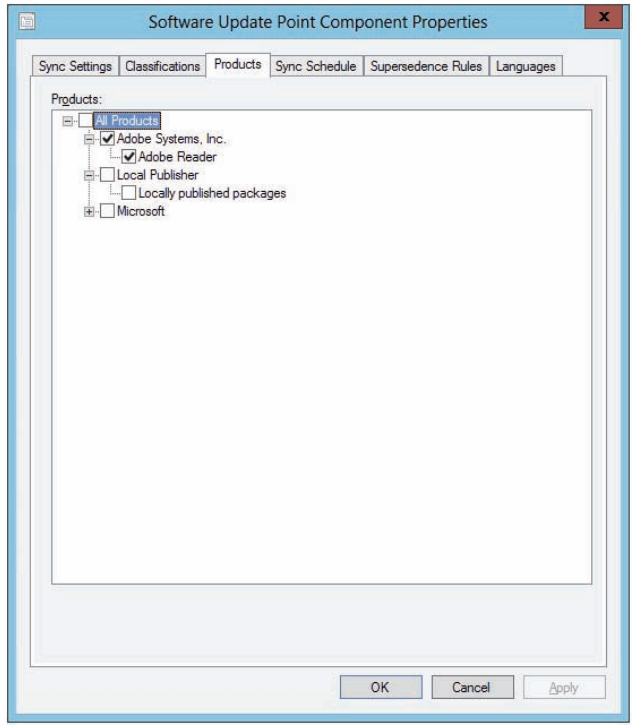
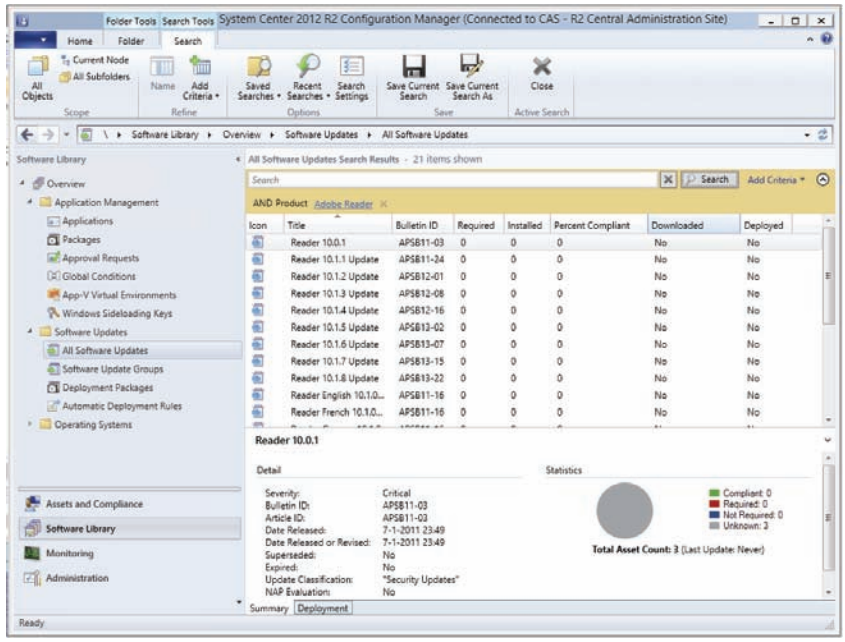


FIGURE 9.40
The third-party updates are available in Configuration Manager.



These updates can be deployed like every other software update in the Software Updates feature.

Monitoring Software Update Deployments

Configuration Manager 2012 offers in-console monitoring. You can see the compliancy level per deployment.

In-Console Monitoring

You can find in-console monitoring of software update deployment in the Configuration Manager 2012 console at several places. The error codes are explained, so you can find the solution instantly.

Monitoring per Software Update

When you select a software update in the All Software Updates repository, the statistics of the software update appear. In the Statistics part of the summary in Figure 9.41, you are able to see how many systems are compliant, how many systems don't need the update, where the update is required, and where the status is unknown.

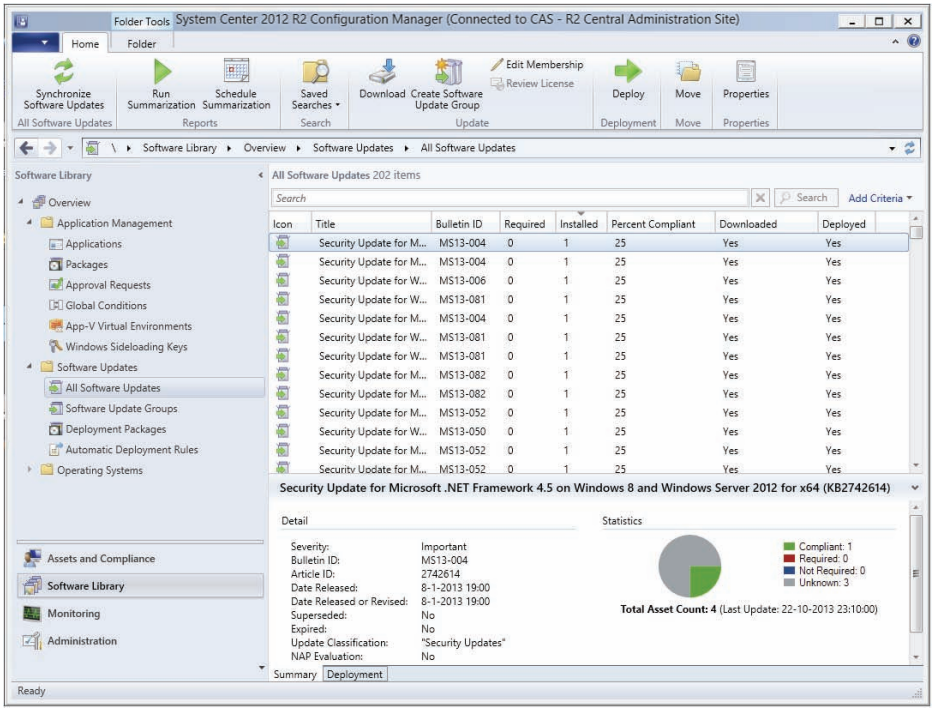


Figure 9.41 In-console statistics per update

Monitoring per Deployment

When you deploy the updates, you can see the deployment status per deployment. The deployment status contains the following categories and subcategories. The deployment status in Figure 9.42 shows how many systems are compliant, how many systems are in the process of installing the updates, how many systems have an error, and where the status is unknown.

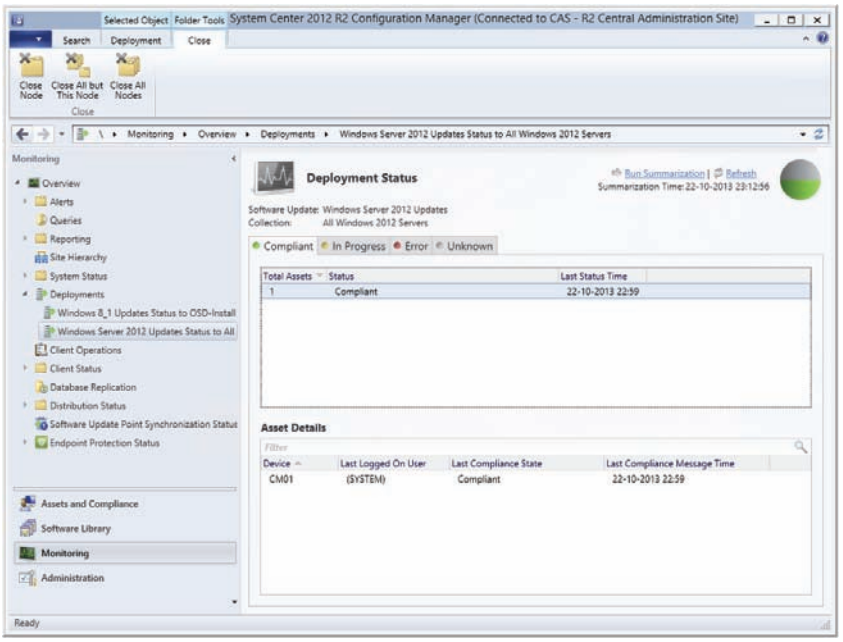


Figure 9.42 In-console statistics per update deployment

Status: Unknown This status says that the status messages of the Configuration Manager clients have not yet been received by the management point of the primary site. The following subcategories are available:

- Devices Unhealthy/Active
- Devices Healthy/Inactive
- Devices Healthy/Active

Status: Error Errors can occur when you deploy software updates. This category shows all the devices that have had an error while deploying the software updates. The following subcategories and error descriptions are available:

- Scan Tool Policy Not Found.
- Network Connection: Windows Update Agent Encountered An Error.
- Policy Platform Client: Data Is Invalid.

- Fatal Error During Installation.
- Pre Install Scan Failed.
- Software Update Still Detected As Actionable After Apply.
- Unknown Error (-2147012744).
- Class Not Registered.
- Access Is Denied.
- Unspecified Error.

Status: In Progress The In Progress status displays all devices that are preparing for the deployment of a software update or are currently receiving a deployment.

The following subcategories are available:

- Downloading Update(s)
- Downloaded Update(s)
- Installing Update(s)

Compliant When the devices are compliant, you will see all the assets that are compliant.

When selecting a system in the Asset Details part of the Deployment Status screen, you can retrieve additional details about the system by right-clicking the system and choosing More Details. In the Asset Manage dialog shown in Figure 9.43, you can view the information about the deployment.

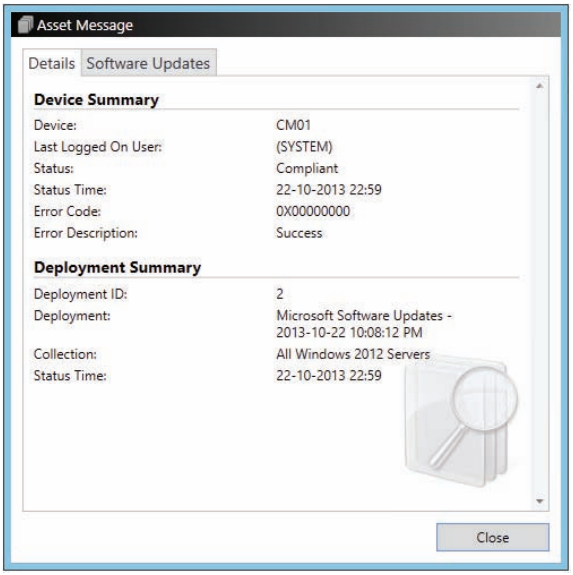


Figure 9.43
Details about the software update deployment

Software Update Point Synchronization Status

Besides examining the log files as described earlier, you can monitor the software update point synchronization status from the console.

To monitor the synchronization in the hierarchy, do the following:

1. In the Configuration Manager console, choose the Monitoring workspace ➢ Overview ➢ software update point Synchronization Status.
2. Examine the synchronization status, the link state, and the catalog version, as shown in Figure 9.44.

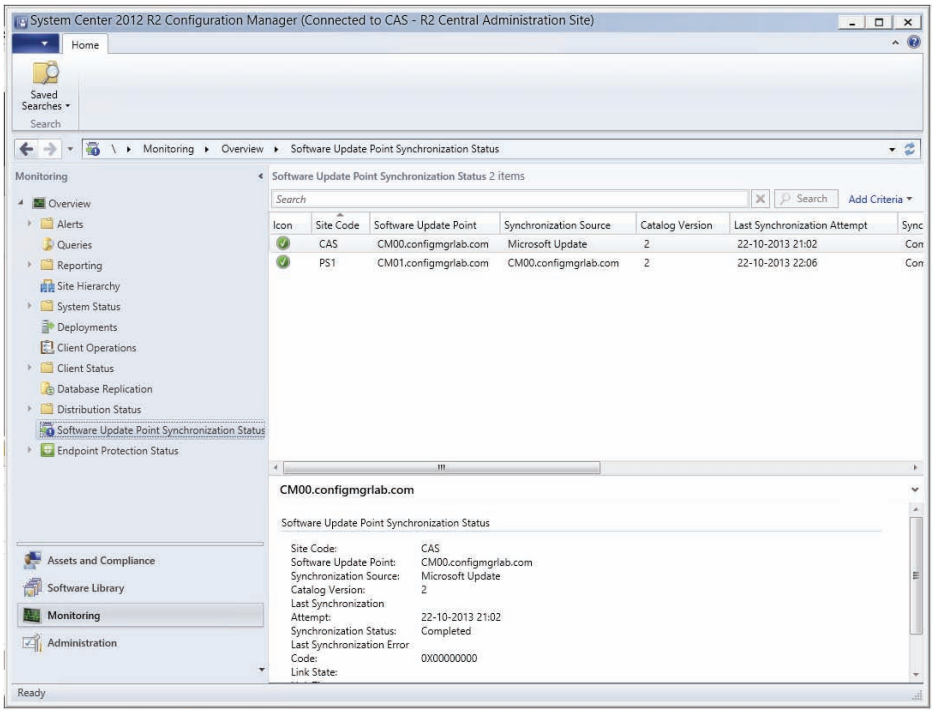


Figure 9.44 Software Update Point Synchronization Status

Reporting

The Configuration Manager client software performs two main phases of the software deployment process:

Evaluation Configuration Manager clients determine if the software updates in a deployment are required.

Enforcement Clients report their compliance state for the deployment.

Microsoft provides excellent reports to monitor the phases of software update deployments in Configuration Manager 2012, and these reports are considered the best way to monitor

the software update deployments. Those reports can be found in the Software Updates - C Deployment States category in the Reports node in the Configuration Manager console.

To monitor the evaluation phase of software update deployments, you should use the following three main reports:

States 2 - Evaluation States For A Deployment This report will give you a summary of the evaluation state of clients for a selected deployment and will provide information as to whether clients were able to evaluate a deployment successfully.

States 4 - Computers In A Specific State For A Deployment (Secondary) You can drill down into this report to get more information about clients in a specified deployment state.

States 7 - Error Status Messages For A Computer (Secondary) You can use this report to get all error message information for a deployment on a specific computer.

To monitor client enforcement for software update deployments, there are also three main reports that you should use:

States 1 - Enforcement States For A Deployment This report gives a summary of the enforcement state of clients for a specific deployment. It shows information on the state for installing the updates in the deployment, such as downloading the update, installing the update, successfully installing the update, and so on.

States 4 - Computers In A Specific State For A Deployment (Secondary) You can drill down into this report to get more information about clients in a specified deployment state.

States 7 - Error Status Messages For A Computer (Secondary) You can use this report to get all error message information for a deployment on a specific computer.



Real World Scenario

Become Familiar with What Needs to Be Updated and Implement Software Updates

Now that you have deployed Configuration Manager and have Software Updates up and running, your manager wants you to make a concentrated effort to get clients up to date with critical security patches. He has made it clear that these are to be given priority over other updates until the numbers of required patches are down to a reasonable level, which is not the case now.

To accomplish your new software update initiative, you must first figure out what patches need to be installed on which computers.

One way to do this is to set up search criteria for each operating system that you support, listing all the critical security patches. With those search criteria, you highlight all the security patches that are required by your clients and make an update group out of them.

Once you have done that, you can either download all the updates and put them on your distribution points, or you can start a deployment directly from the update group and configure downloading those updates as part of that update.

The procedures that we have detailed earlier in the chapter for configuring the different elements of Software Updates were made with that method of organization in mind.

The Bottom Line

Plan to use Software Updates. You can use the same method of deployment intelligence that was used in Chapter 2 to gather information for planning to implement Software Updates. This will be very helpful in making sure that you get the most out of the Software Updates feature for your organization.

> **Master It** What is the first step in gathering deployment intelligence when you are planning to implement Software Updates?

Configure Software Updates. Before you can utilize Software Updates in your environment, you must set up and configure the various components of this feature.

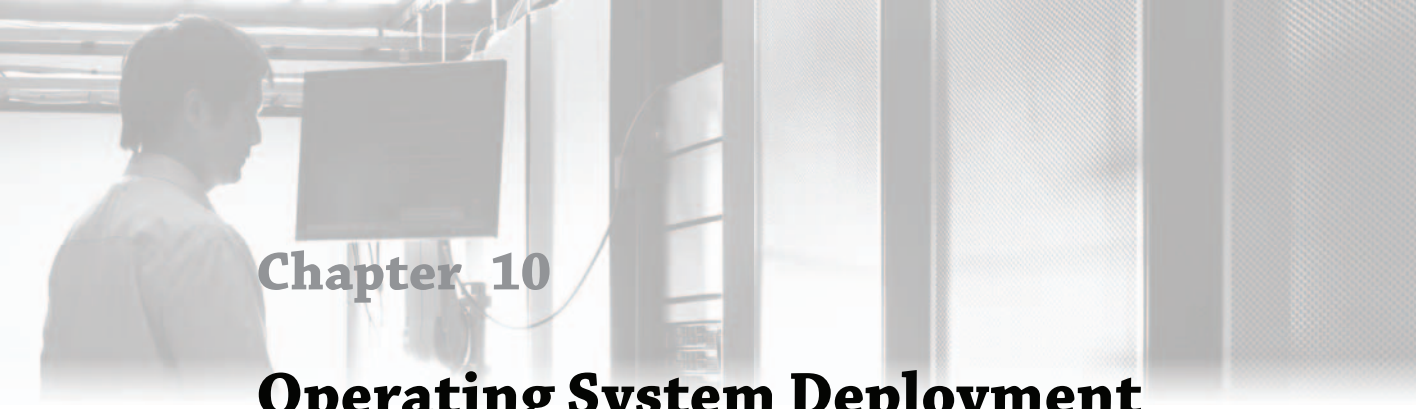
> **Master It** What is the first thing you have to install before you can use Software Updates?

Use the Software Updates feature to manage software updates. The hardest thing to do in SMS 2003 relating to patch management was to programmatically prioritize software updates that are critical so they can be deployed with a higher priority than other updates.

> **Master It** What does Configuration Manager provide that can help with prioritizing software updates?

Use automatic update deployment to deploy software updates. When you deployed software in Configuration Manager 2007, you deployed software updates through a procedure that consumed a lot of time.

> **Master It** Configuration Manager has a new feature called Automatic Deployment Rules. What kinds of updates are suitable to deploy via the automatic deployment rules?



Chapter 10

Operating System Deployment

Most IT administrators want to automate as many functions as possible in order to reproduce the same outcome consistently and quickly to as many devices as possible, and setting up a basic computer build is no exception.

In Configuration Manager 2007 the operating system deployment (OSD) feature became one of the most important features of Configuration Manager. With Configuration Manager 2012 you can install Windows operating systems without any user intervention. We call this Zero-Touch deployment. When a Windows deployment is finished, the user is able to log into the network and start working with the new operating systems and the available applications. The operating system deployment feature is highly dependent on the Windows Assessment and Deployment Kit (ADK) for Windows 8.1. The Windows ADK is a prerequisite of Configuration Manager 2012 R2.

In Configuration Manager 2012 the operating system deployment feature matured with added features such as offline servicing. We will walk you through several Windows deployment scenarios without and with the use of the Microsoft Deployment Toolkit 2013.

In this chapter, you will learn to

- Specify a Network Access account
- Enable PXE support
- Update the driver catalog package
- Update an image from the console

What's New in Operating System Deployment

The operating system deployment feature in Configuration Manager 2012 was not significantly changed from Configuration Manager 2007. Nevertheless some parts are enhanced, changed, or new to the feature. The following list shows the changes since Configuration Manager 2007:

- The Preboot Execution Environment (PXE) role was moved from the primary site server to the distribution point. This way scalability is increased since it is easier to deploy an extra distribution point.
- Updating a WIM image with the latest approved software updates is done from the Configuration Manager console.
- You can use task sequence media to deploy operating systems anywhere in your Configuration Manager hierarchy.

- A boot image is available throughout the Configuration Manager hierarchy instead of needing to deploy a boot image in every site.
- The Create Task Sequence Media Wizard provides the option to add prestart command files to prestage media, stand-alone media, and bootable media.
- You can configure the task sequence media to become unattended installation media by suppressing the Configuration Manager Boot Media Wizard during the installation.
- In the task sequence, a capture user state task or restore user state task supports the new features of the User State Migration Tool (USMT) version 4.
- From the task sequence you can install applications from the new application model.
- Configuration Manager 2012 supports deploying Windows To-Go devices.
- Configuration Manager 2012 supports deploying and uploading virtual hard disks to System Center 2012 R2 Virtual Machine Manager (VMM).

Planning for OSD with Configuration Manager 2012

Before you configure the feature, you should plan your operating system deployment, since you can deploy different kinds of operating systems in numerous ways. To deploy your operating systems in an effective and cost-efficient way, you need to address the following items when planning your operating system deployment:

- Deployment scenarios
- The kind of images to deploy
- The kind of components to use

Deployment Scenarios

You can deploy the operating system in different ways. In Configuration Manager 2012 you can deploy an operating system in two kinds of scenarios:

Bare-Metal Scenario Installing an operating system to a new out-of-the-box client computer

Refresh Computer Scenario Deploying an image to an existing Windows installation to perform an upgrade or reinstall while migrating the user state to the new Windows installation

The Kind of Images to Deploy

Configuration Manager 2012 supports, as did the previous version of Configuration Manager, the deployment of two kinds of operating system installations. You can install images, based on the Windows Imaging (WIM) format, or just install operating systems by using the source of an operating system installation. Using the source of an operating system is an unattended installation and is normally used to create a WIM image with a build-and-capture task sequence. The source can be a copy of the DVD of Windows 8.*x*, Windows 7, Windows Vista, Windows XP SP3, Windows Server 2003, Windows Server 2008 (R2), or Windows Server 2012 (R2).

Operating System Images Operating images are often custom images that are built with the build-and-capture task sequence. This task sequence allows you to install and create an image of a customized reference operating system image. Also, the operating system images are used when you want to build and capture a custom image of a Windows 7 or higher or a Windows Server 2008 or higher operating system.

Operating System Installer An installer source is used as the source for a build and capture to perform an unattended installation of legacy operating systems like Windows XP and Windows Server 2003 before capturing it to a WIM image.

Operating System Deployment Components

The operating system deployment feature uses different kinds of components within Configuration Manager 2012. We'll look at each of them.

Boot Images

Configuration Manager 2012 comes with two default boot images. These images are available for all sites in the hierarchy. There is no need to create and deploy boot images for each Configuration Manager site in the hierarchy.

When you access a standard boot image, you can configure several settings in various tabs. To access the boot image, browse to the Software Library workspace ➢ Overview ➢ Operating Systems ➢ Boot Images. The tabs shown in Figure 10.1 are available.

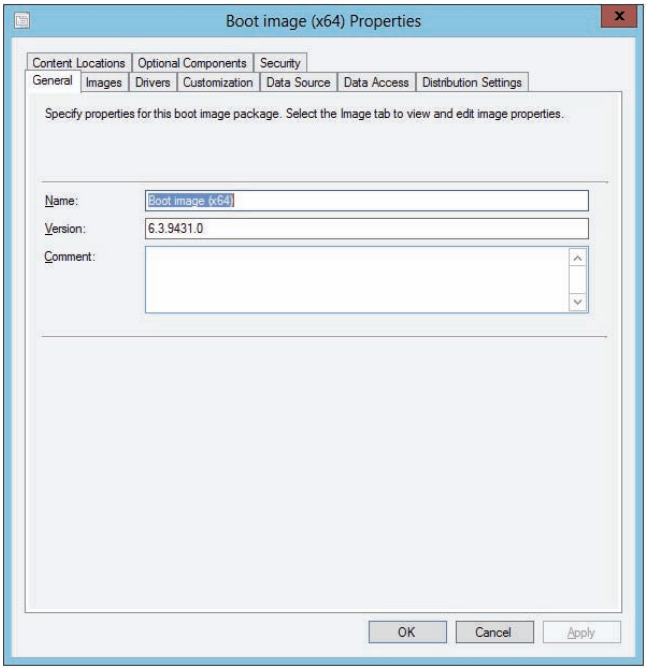


Figure 10.1 Boot Image Properties

General Tab In the General tab, you can enter or change the name, version, or comments of the boot image that's already available in Configuration Manager 2012.

Images Tab The Images tab provides information about the boot image. If you changed the image properties with an external tool, you can reload the original properties.

Drivers Tab The Drivers tab provides an overview of the drivers that are injected into the boot image. You can also add drivers from the driver store to the boot image. Common drivers to add to boot images are network and SATA/SCSI drivers and any other critical drivers.

Customization Tab If you want to customize the selected boot image, you can find some options on the Customization tab. When you're in the plan and build phases of your project and you want to test the deployment of images, you can enable command support in the Windows Preinstallation Environment (WinPE) phase of your deployment. Pressing F8 opens a command prompt that allows you to access the file system and log files that are located in the `_SMSTaskSequence\Logs\Smstslog` directory. There is also an option to change the background that is shown during the WinPE phase.

If you want to add a prestart command hook and supporting files, you can add the command line here.

Data Source Tab The Data Source tab supplies the path to the boot WIM image that is used for the boot image package. The Data Source tab is also the place to enable or disable the ability to boot the image from PXE.

Data Access Tab With settings in the Data Access tab you can configure how the package is stored on the distribution points.

Distribution Settings Tab Here you can define how the boot image package is distributed to the distribution points and set the priority.

Content Locations Tab On the Content Locations tab you can see on which distribution points or distribution point groups the image package is available. Selecting a distribution point or distribution point group allows you to validate the copy on the location, redistribute the boot image package to the location, or remove the boot image package from the location.

Optional Components Tab In earlier versions you would definitely create new boot images with the Microsoft Deployment Toolkit to be able to use advanced features within WinPE. Configuration Manager 2012 R2 adds the ability to add optional components to the WinPE images from the Configuration Manager console.

Security Tab The Security tab shows you the users who have administrative permissions to the boot image object.

Deciding When to Use Which Boot Image

There are two different versions of boot images to support two kinds of platforms, namely an x86 version and an x64 version.

You can use the x86 boot image version to deploy the following:

- 32-bit operating system image
- 64-bit operating system image
- 32-bit operating system install package

You can use the x64 boot image version to deploy the following:

- 64-bit operating system image
- 64-bit operating system install package

You can define per task sequence which boot image to use.

State Migration Point

The state migration point stores the user data that is gathered by USMT when a computer is being refreshed by a new Windows operating system. The component can be configured to store user data on different storage folders, depending on the deletion policy.

Distribution Points

The distribution point is used to store the content that is related to the operating system deployment. But in Configuration Manager 2012 two very important features have been moved to the distribution point, namely PXE and multicast.

When configuring a distribution point for operating system deployment, you can adjust the following settings:

PXE Tab As mentioned earlier, the PXE feature has been moved to the distribution point. The PXE tab allows you to enable or disable support for PXE, but a Windows Deployment Services service must be present. As in earlier versions, you can configure PXE to respond to incoming PXE requests and unknown computer support. New is the ability to enable Primary User Assignment, which is discussed later in this chapter. If you want to secure PXE with a password, you can configure one. When you enable a boot image for PXE and the boot image is available on the distribution point, the boot image is also copied into the `RemoteInstall\SMSBoot` folder of Windows Deployment Services. Enabling the PXE feature will also install the Windows Deployment Services feature if the feature is not yet available.

Multicast Tab The Multicast feature has also been moved to the distribution point via PXE. You configure the options per distribution point.

Operating System Images

The operating system images are the WIM images that can be deployed to workstations or servers. An operating system image can be a captured operating system. When you access an operating system image, you can configure several settings in various tabs. To access an operating system image, go to the Software Library workspace ➢ Overview ➢ Operating Systems ➢ Operating System Image.

General Tab The General Tab is used to supply information about the operating system image, like name, version, and comments.

Images The Images tab gives you information about the WIM image. Information like OS version, architecture, creation date, and more is shared. If you changed the image properties using an external tool, you can reload the information from the WIM image.

Data Source Tab The Data Source tab supplies the UNC path to the WIM image that is used for the operating system image package.

Data Access Tab With settings in the Data Access tab you can configure how the package is stored on the distribution points.

Distribution Settings Tab Here you can define how the operating system image package is distributed to the distribution points and set the priority. You are also able to define to allow this operating system image to be transferred via multicast via WinPE.

Servicing In the Servicing tab you are able to see or change the offline servicing schedule if offline servicing for an image is scheduled.

Installed Updates The installed updates tab gives you a list with installed updates that have been installed with offline servicing.

Content Locations Tab On the Content Locations tab you can see on which distribution points or distribution point groups the operating system image package is available. Selecting a distribution point or distribution point group allows you to validate the copy on the location, redistribute the operating system image package to the location, or remove the operating system image package from the location.

Security Tab The Security tab shows you the users who have administrative permissions to the operating system image object.

Operating System Installers

The operating system installers are the install source of an operating system. With the operating system installers you are able to install operating systems unattended. Operating system installers are used, for instance, while building and capturing an operating system image. When you access an operating system installer, you can configure several settings in various tabs. To access an operating system installer package, go to the Software Library workspace ➢ Overview ➢ Operating Systems ➢ Operating System Installers. Operating system installers for Configuration Manager 2012 R2 are supported only for Windows 8.*x*. For earlier versions of Windows, you need to add custom boot images based on the Windows Automated Installation Kit.

General Tab The General Tab is used to supply information about the operating system installer, like name, version, and comments.

Editions The Editions tab allows you to see information about the selected edition in the installation source. For instance, a Windows Server 2008 R2 install source has more editions available; editions can be Standard, Enterprise, or Datacenter.

Data Source Tab The Data Source tab supplies the UNC path to the install source of the operating system installer that is used for the operating system installer package.

Data Access Tab With settings in the Data Access tab you can configure how the package is stored on the distribution points.

Distribution Settings Tab Here you can define how the operating system installer package is distributed to the distribution points and set the priority.

Content Locations Tab On the Content Locations tab you can see on which distribution points or distribution point groups the operating system installer package is available. Selecting a distribution point or distribution point group allows you to validate the copy on the location, redistribute the operating system installer package to the location, or remove the operating system installer package from the location.

Security Tab The Security tab shows you the users who have administrative permissions to the operating system installer object.

Task Sequences

Task sequences provide a mechanism to perform a series of tasks on a client computer without any user intervention. Using task sequences, you can deploy operating systems but also distribute software, configure client settings, update drivers, edit user states, and perform other tasks in support of operating system deployment. Task sequences are global data and are available for all Configuration Manager sites in the hierarchy.

With Configuration Manager 2012, you can create four different kinds of task sequences:

Install An Existing Image Package This task sequence will install an existing WIM image to a computer via the normal distribution method or PXE. This option uses a predefined sequence of steps. The steps will take care of wiping or formatting the disk, installing the operating system, installing software updates, installing applications, and setting the user state.

Build And Capture A Reference Operating System Image This task sequence will build and capture a Windows operating system in a new WIM image. You can use this WIM image to deploy to the client computers. This option uses a predefined sequence of steps.

Install An Existing Image Package To A Virtual Hard Drive This task sequence will install an existing image package and shut down the computer. This task sequence is used with the Create Virtual Hard Drive Wizard. The wizard creates a temporary virtual machine, creates the virtual hard drive, installs task sequence, and saves the virtual hard drive to a defined location. The Create Virtual Hard Drive Wizard is discussed later in this chapter in detail.

Create A New Custom Task Sequence A custom task sequence is an empty task sequence for which you define your own steps.

A task sequence consists of tasks or steps grouped into the following categories:

General In the General category the following tasks can be configured for the task sequence:

- Run Command Line
- Run PowerShell Script
- Set Dynamic Variables
- Install Application
- Install Package
- Install Software Updates
- Join Domain Or Workgroup
- Connect To Network Folder
- Restart Computer
- Set Task Sequence Variable
- Check Readiness

Disks In the Disks category the following tasks can be configured for the task sequence:

- Format And Partition Disk
- Convert Disk To Dynamic
- Enable BitLocker
- Disable BitLocker
- Pre-provision BitLocker

User State In the User State category the following tasks can be configured for the task sequence:

- Request State Store
- Capture User State
- Restore User State
- Release State Store

Images In the Images category the following tasks can be configured for the task sequence:

- Apply Operating System Image
- Apply Data Image
- Setup Windows And ConfigMgr
- Install Deployment Tools
- Prepare ConfigMgr Client For Capture
- Prepare Windows For Capture
- Capture Operating System Image

Drivers In the Drivers category the following tasks can be configured for the task sequence:

- Auto Apply Drivers
- Apply Driver Package

Settings In the Settings category the following tasks can be configured for the task sequence:

- Capture Network Settings
- Capture Windows Settings
- Apply Network Settings
- Apply Windows Settings

Task Sequence Media

When you use task sequence media, you can create a CD, DVD, or USB containing the files required for deploying or capturing an operating system with Configuration Manager. You can select the following kinds of media:

Stand-Alone Media Use this type of media to deploy an operating system without network access.

Bootable Media Use this type of media to access the Configuration Manager 2012 infrastructure to deploy an operating system across the network.

Capture Media Use this type of media to capture a WIM image of an operating system on a reference computer.

Prestaged Media Use this type of media to create a file for operating system deployment that contains an operating system image and bootable media that can be prestaged on a hard disk.

Driver Catalog

The driver catalog is the place to store device drivers that need to be added during a Windows deployment or to a boot image. Normally not all the device drivers need to be added, because Windows 8 supports many hardware platforms and devices. When you deploy an operating system, you can include a driver package or let WinPE discover the drivers through WMI.

You can organize your driver structure by adding the drivers for each make and model to folders or categories. This way you can clean up old drivers in the future.

Driver Packages

The driver packages are used to keep the drivers grouped per brand, model, operating system, and/or platform. These driver packages need to be distributed to the distribution point (groups) in your Configuration Manager hierarchy.

User Device Affinity

User device affinity helps you create relationships between users and devices. You create relationships by either adding primary devices to users or by adding primary users to devices. When you deploy a new operating system to a device, Configuration Manager 2012 will check the user's collection memberships and predeploy the user-targeted applications. The user's primary device will attempt to install the application that is targeted to the user whether or not the user is logged on.

Configuration Manager 2012 allows you to create the following relationships:

- Single primary user to primary device
- Multiple primary devices per user
- Multiple primary users per device

Deployment Process

When you deploy a Windows operating system using the task sequences of Configuration Manager, you need to follow certain steps to be sure that the deployment will succeed. Generally speaking, there are three major steps to deploy an operating system: prepare, build and capture, and deploy.

Prepare for Operating System Deployment

The first step is preparing the Configuration Manager environment so that you can deploy the operating system. Gather the information that you need to create an image of an operating system and deploy it to client computers. Essential information includes the makes and models of the computers and the devices that need drivers. You also need to incorporate whether you want to add applications to the image or not.

Build and Capture an Operating System

After your design for the operating system is finished, you need to translate the design into a task sequence that will build and capture your operating system.

The build-and-capture task sequence creates a fully unattended installation of a Windows operating system. Depending on your design, the task sequence can take care of installing the available software updates and, if you like, applications that are part of the common operating environment. Incorporating applications into your WIM image is not a best practice, but there are situations where you'll want to add some applications to your image.

Another option is to use a reference computer and capture the reference operating system, which is created manually, using a capture media task sequence.

Fat vs. Thin Images

When you deploy Windows images in your environment, think about how to deploy your common operating environment, operating system, and standard applications. You can choose to deploy your operating system and applications in an image (fat image) or just the operating system in an image (thin image) and the applications during the deployment process. A thin image is easier to maintain because you don't have to recapture your image when an application needs to be updated. However, a fat image may be quicker to deploy.

Deploy an Operating System

After capturing an operating system image, you can deploy it to one or more computers in your environment. The task sequence that you create can be used for bare-metal deployment or to refresh or upgrade a computer that is a member of an existing Configuration Manager 2012 environment. After creating a task sequence to deploy your Windows image, you can change and add tasks to suit your needs. You can also add or change the software updates, installation of applications, disk layout, domain, network settings, and much more.

Maintaining Images

Configuration Manager 2012 supports maintaining your Windows images with software updates from the console. You can schedule offline servicing of the Windows image by adding the latest software updates and redeploying the images to your distribution points periodically. This is described in the section "Servicing Your Operating System Images and VHDs Offline" later in this chapter. It is recommended that you re-create your image every quarter; this way you will keep your images up to date and the deployment process fast and smooth.

Preparing Configuration Manager 2012 for Operating System Deployment

You need to configure Configuration Manager 2012 for deploying an operating system image. The first step in preparing for OSD is to configure the Network Access account. Then you need to install and configure the state migration point role and enable the PXE feature on the distribution points. In earlier versions of Configuration Manager you had to manually create packages for the Configuration Manager Client and the User State Migration Tool; in Configuration Manager 2012 R2 those packages are available by default after the installation of Configuration Manager 2012 R2.

Configuring the Network Access Account

The first step is to set up an Active Directory user as the Network Access account. As mentioned in Chapter 8, "Application Deployment," you are able to create more than one Network Access account to support, for instance, multiple forests. A general rule for those accounts is to give them an easily identifiable name. For example, a domain administrator would create an account called svc-sccm-na (or whatever fits your environment's naming conventions).

Next, you will need to configure Configuration Manager 2012 to use the Network Access account. Take the following steps:

1. Open the Configuration Manager 2012 console, choose the Administration workspace, and expand Overview ➢ Site Configuration ➢ Sites.
2. Select one of the sites for which you want to configure the Network Access account, and click Configure Site Components in the settings section on the Home tab of the ribbon.
3. Select Software Distribution.
4. Select the Network Access Account tab, and set the Network Access account to the account created earlier, as shown in Figure 10.2.
5. Click OK.

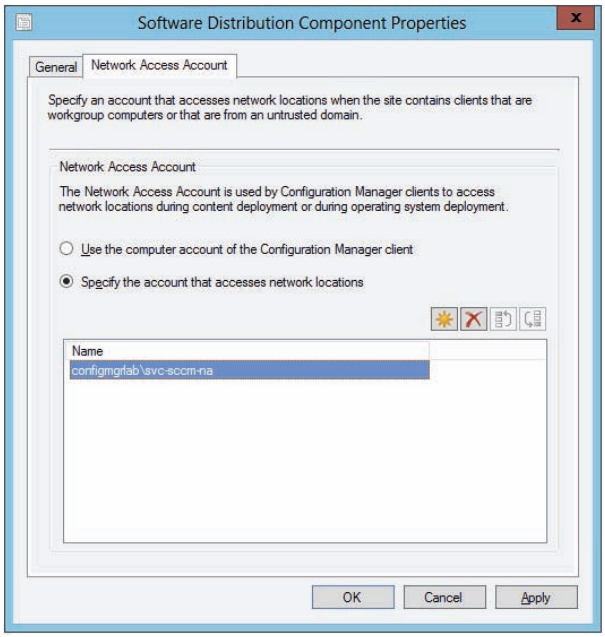


FIGURE 10.2
Software Distribution Component Properties dialog box

The Network Access account must have access to the computer that is deployed and to the content on the distribution points. Normally a Network Access account has permission if it's a member of the Domain Users Active Directory group.

Configuring the State Migration Point Role

The next step in preparing Configuration Manager 2012 for OSD is to set up a state migration point. The state migration point is used to store user-migrated settings and data during the operating system image deployment. This state migration point is a site system role within Configuration Manager 2012, and it will need to be assigned to a server. Follow these few steps to set up the state migration point role:

1. Open the Configuration Manager 2012 console, select the Administration workspace, and expand Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Select the site server for which you want to install and configure the state migration point, and click Add Site System Roles on the Home tab of the ribbon.
3. On the Add Site System Roles Wizard's General page, click Next twice.
4. You will be presented with the System Role Selection page; select State migration point, and click Next.
5. On the State Migration Point page, shown in Figure 10.3, click the starburst icon to create a new storage folder.

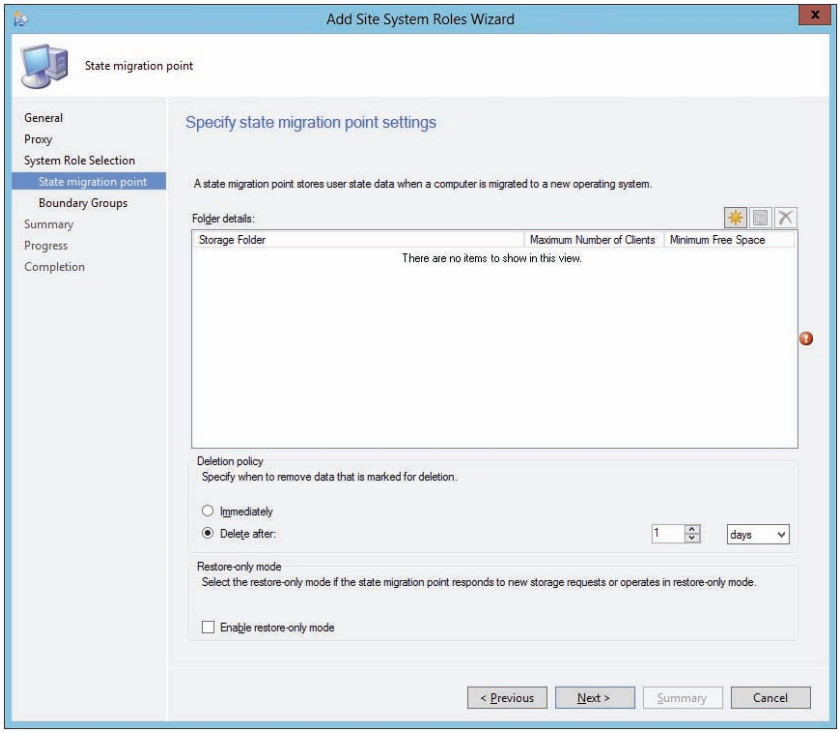


FIGURE 10.3
Add Site System Roles Wizard—State Migration Point page

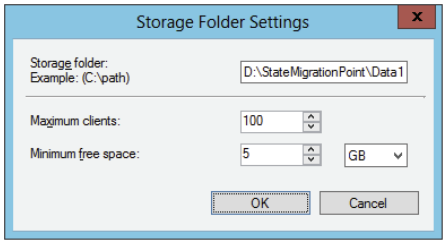


FIGURE 10.4
Designating a storage folder

6. Create a new storage folder in the Storage Folder Settings dialog, shown in Figure 10.4.

   This allows you to enter the path to use when storing state migration data.

7. Under the storage folder you also need to configure the maximum number of clients that are allowed to store the data and the minimum required free space on the disk.

A way to determine the size for your state migration point is to identify the number of deployments that must take place, the average size of the user state, and how long the user state must be stored. Be sure to keep your drive from running out of free space by configuring a minimum free space for the disk where the storage folder is located.

8. Click OK to return to the State Migration Point page.

   You can change the Deletion Policy setting if you think one day is too long or not long enough until the user data is removed from the state migration point.

   Enabling the Restore-Only Mode option will result in the state migration point responding only to restore requests.

9. Click Next to configure boundary groups for the site system.
10. Click Next, and you will be taken to the Summary page.
11. Click Next to allow Configuration Manager to create the new site role.

    This brings up the Wizard Completed page.

12. Click Close.

Don't Configure the Deletion Policy to Delete User State Immediately

A best practice from Microsoft is not to set the deletion policy to delete a user state immediately after it is marked for deletion. If an attacker is able to retrieve the user state before a valid computer does, the user state would be deleted before that time. Set the deletion interval to long enough to verify the successful restore of the user state data.

Configuring PXE on Distribution Points

To allow Configuration Manager 2012 to use OSD for deploying to bare-metal devices, you need to configure PXE on the distribution points, for which you will need to set up the Network Access account, which you did earlier in this chapter. You will also need to ensure that the Configuration Manager client upgrade package has been configured and is ready for deployment, as you also did earlier in this chapter. Finally, you need to ensure that the boot image is set up as a package.

To be able to use PXE on a distribution point site server, you also need to install Windows Deployment Services (WDS) on that server.

Installing Windows Deployment Services

You can install Windows Deployment Services through Add or Remove Programs on Windows 2003 SP2 or higher machines. If you do not install the Windows Deployment Services feature within Windows, Configuration Manager 2012 will automatically install this feature when enabling the PXE feature on the distribution point.

The next stage in preparing Configuration Manager 2012 for OSD is to set up PXE support. Configuration Manager no longer has a PXE service point; the PXE feature is embedded in the distribution point role. You need to enable and configure the PXE feature per distribution point.

Follow these few steps to set up the PXE feature:

1. Open the Configuration Manager 2012 console, select the Administration workspace, and expand Overview ➢ Distribution Points.
2. Select the site server on which the distribution point resides, and click Properties on the Site Role tab of the ribbon.
3. Select the PXE tab and click Enable PXE Support For Clients.

   When you enable the feature, you will see a Review Required Ports For PXE dialog box, shown in Figure 10.5. This dialog box informs you that Configuration Manager 2012 must have some UDP ports opened on the server.

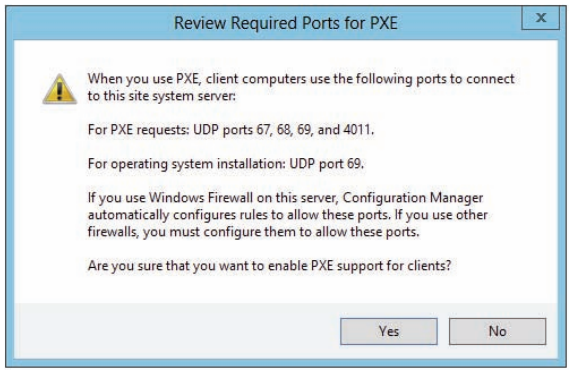


FIGURE 10.5 Review Required Ports For PXE dialog box

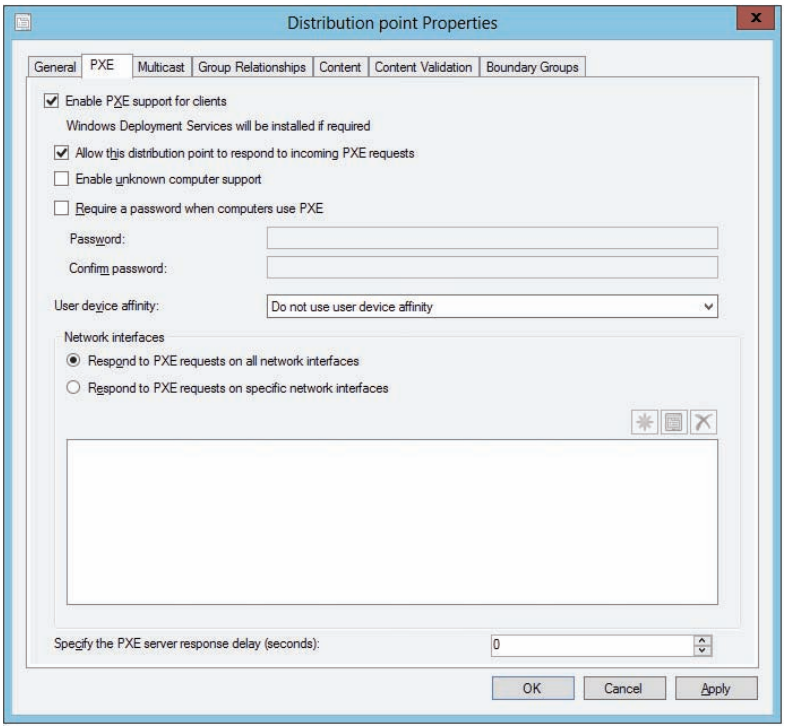
4. Click Yes to continue enabling PXE support for clients.
5. After enabling the feature, you can configure how Configuration Manager will allow incoming PXE requests, as shown in Figure 10.6. Click OK when you've finished.

It will take some time for the PXE feature to successfully install on the system. You can monitor the progress of the installation by checking the `distmgr.log` and `smspxe.log` files. Windows Deployment Services will be installed if it is not already present on this system.

DHCP and PXE on the Same Server

You'll need to set up some DHCP options for PXE to boot properly. Specifically, you'll need to specify options 60, 66, and 67 when the DHCP server is on the same server as your Windows deployment server. Option 60 needs to be set to PXEClient, which is only used in this scenario. Option 66 is the FQDN of the Configuration Manager server, and option 67 should be the path to `SMSBoot\<platform>\pxeboot.com`.

FIGURE 10.6
PXE settings page



Distributing the Boot Image Package

The next part of preparing Configuration Manager 2012 for operating system deployment is to distribute the boot image package to a distribution point. This boot image is used to start the computer in the Windows Preinstallation Environment (WinPE) for capturing, prior to deploying the operating system image. This procedure, because of the size of the images, will take some time to complete:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Boot Images.

   You will notice two boot images for various platforms: one for x64—Boot Image (x64)—and the other for x86 devices—Boot Image (x86). For the purpose of this book, we will concentrate on the x86 boot image, but there is basically no difference in configuring one or the other. The images are configured during the installation of Configuration Manager 2012. However, there are no distribution points assigned for either of the boot images. You need to add both Boot Image Packages to the distribution points.

2. To configure a distribution point, select Boot Images ➢ Boot Image (x86), and click Distribute Content on the Home tab of the ribbon.

3. This opens the Distribute Content Wizard's Welcome page; click Next to continue.

4. Select the distribution point you want to use on the Specify The Content Destination page by clicking Add ➢ Distribution Point.
5. Select the distribution points you want to deploy the boot image to, and click OK.
6. Click Next to review the summary.
7. After reviewing the summary, click Next. Then on the Wizard Completed page, click Close.

   It will take some time to copy the boot image package to the distribution point. Do the same for the boot image called Boot Image (x64).

Enabling Boot Images for PXE

The last part of preparing Configuration Manager 2012 for OSD is enabling both of the boot images to be available for PXE:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Boot Images.
2. Select the boot image for which you want to enable PXE support, and click Properties on the Home tab of the ribbon.
3. Click the Data Source tab, and enable the Deploy This Boot Image From The PXE-Enabled Distribution Point option, as shown in Figure 10.7.
4. Click OK.

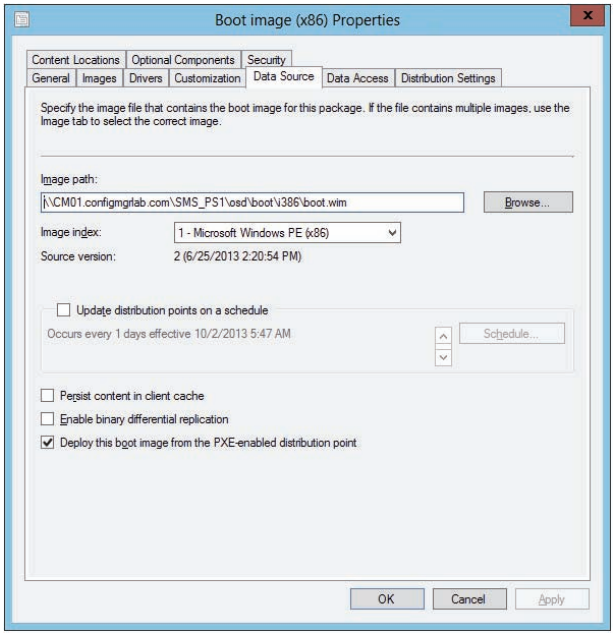


FIGURE 10.7 Enable the boot image to boot via PXE

Configuration Manager will process the change and configure the Windows Deployment Services server to use the boot image from Configuration Manager 2012. Configuration Manager 2012 will place the boot image in the `<drive>\RemoteInstall\SMSImages` folder.

Let's review the steps briefly for configuring Configuration Manager 2012 for OSD:

1. First, you configure the Network Access account, and then you create the client install package.
2. Second, you set up the state migration point and PXE support for Configuration Manager 2012.
3. Finally, you deploy the boot images to the distribution points and PXE-enabled distribution points.

Adding Operating System Source

The next step after preparing Configuration Manager 2012 for OSD is to add the source content of the default operating systems. Adding a source of an operating system that you can use for the build and capture process can be done in two ways:

Adding an Operating System Package The operating system install packages can be used to build and capture a reference image that you can deploy with Configuration Manager 2012 by using the setup. With Configuration Manager 2012 R2 and the default boot images, only Windows 8.*x* operating system installers are supported. To be able to build and capture earlier versions, boot images based on the Windows Automated Installation Kit must be created and added to Configuration Manager. Adding legacy boot images is covered later in this chapter. Using the Build And Capture Task Sequence Wizard will give you the only option of selecting an operating system image. You need to change the task sequence step that installs the operating system image after the task sequence is created.

Adding a Default INSTALL.WIM image as an Operating System Image Another way is to add the default `INSTALL.WIM` as an operating system image to Configuration Manager. The `INSTALL.WIM` file can found in the source of the DVD or ISO that holds the operating system. The Build And Capture Task Sequence Wizard lets you select the operating system image directly.

You can add an operating system install source package by following the next procedure:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Installers.
2. Click Add Operating System Installer on the Home tab of the ribbon, and fill in the UNC path to the install source of the operating system, as shown in Figure 10.8.
3. Click Next.
4. Supply the operating system install package with a name, version, and comments, and click Next.
5. Review the summary, and click Next.
6. When finished, click Close.

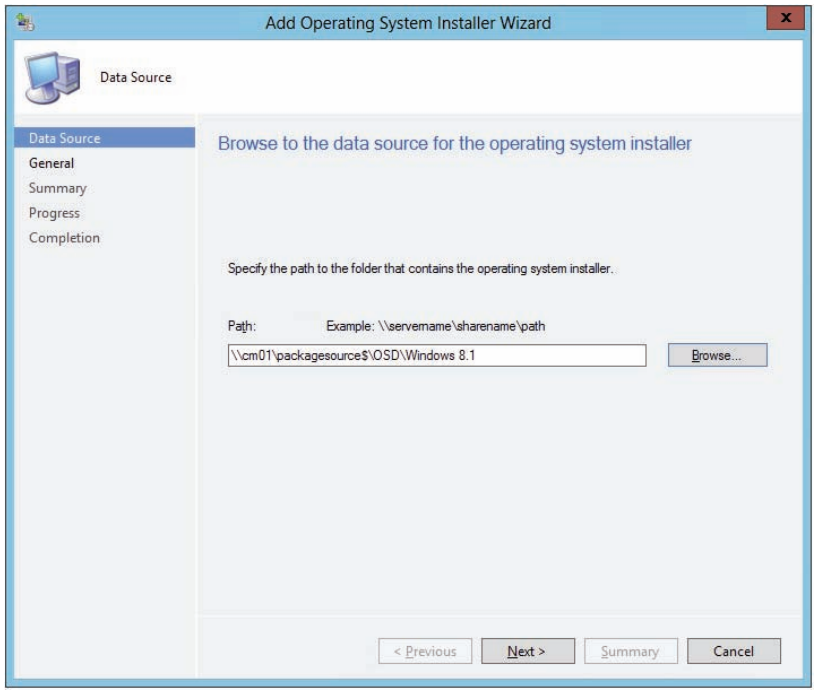


FIGURE 10.8
Create an operating system install package

After creating the operating system installer package, distribute the package to select distribution points in your hierarchy. The source of an operating system install package in combination with the default boot images can be one of the following operating systems:

- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

You can add an `INSTALL.WIM` file from an operating system source by following the next procedure:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Images.
2. Click Add Operating System Image, and browse to the root UNC location of the install source on your package source share. From there browse to Sources and select the `INSTALL.WIM` file, as shown in Figure 10.9.

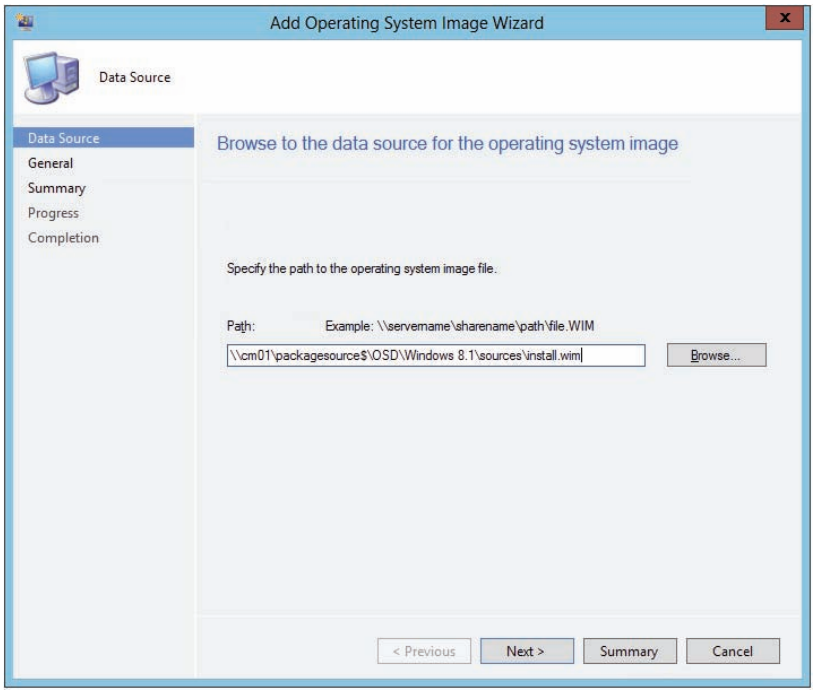


FIGURE 10.9 Add an `INSTALL.WIM` file as an operating system image.

3. Click Next and supply the operating system image with a name, version, and comments if necessary, and click Next again.
4. Review the summary, and click Next.
5. When finished, click Close.

After creating the operating system image package, distribute the package to the distribution points in your hierarchy. By using this method, you can build and capture the following operating systems:

- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Developing a Task Sequence for Creating a Capture Image

Now we will show how to create a task sequence that will be used to capture an image of a workstation. A *task sequence* is a way for Configuration Manager 2012 to perform one or more steps or tasks on a client computer without requiring user intervention, also known as Zero-Touch deployment. A task sequence can consist of a single step or multiple tasks grouped together to perform functions. The tasks can depend on other tasks to complete successfully or be independent of each other.

There are two options for creating task sequences for OSD:

- Task sequences used with PXE boot
- Task sequences used with media boot

Task Sequences Used with PXE Boot

When you enable PXE on the distribution points, you can simply create a build-and-capture task sequence that will take care of the build-and-capture process. Take the following steps to create a task sequence for creating an image:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Click Create Task Sequence on the Home tab of the ribbon, and select the Build And Capture A Reference System Image option.
3. Give the task sequence a name (for instance, Build And Capture Windows 8.1 Enterprise), select a boot image that will support your operating system version and platform, and click Next.
4. Select the operating system image package, and supply a password that you will remember if you need to troubleshoot. Selecting the operating system image is the default; if you want to use the operating system installer, you need to change the task sequence after the wizard is finished.

   The local administrator account will be disabled if you do not supply a password.
   Do not supply a product key if you are building and capturing Windows 7, Windows 8.*x*, Windows Server 2008, or Windows Server 2012 images, as shown in Figure 10.10. Supplying a product key while building and capturing will cause the process to fail with exit error 31.
5. Click Next to move to the next page of the wizard.
6. Supply a name for the workgroup that you want to join while you are building and capturing your operating system.

   Be sure to join a workgroup so that no Group Policies are applied while you are building and capturing your reference image.
7. Click Next after supplying the name of the workgroup.

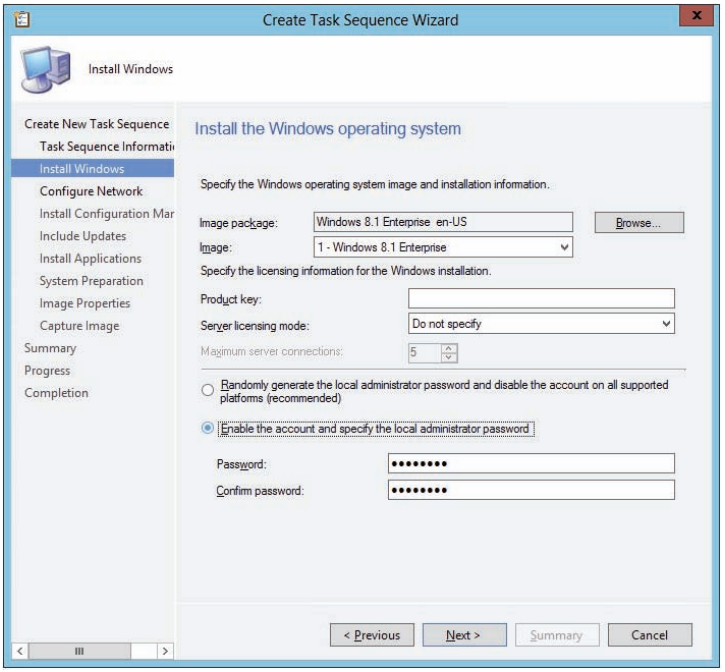


FIGURE 10.10
Define which Windows operating system will be captured.

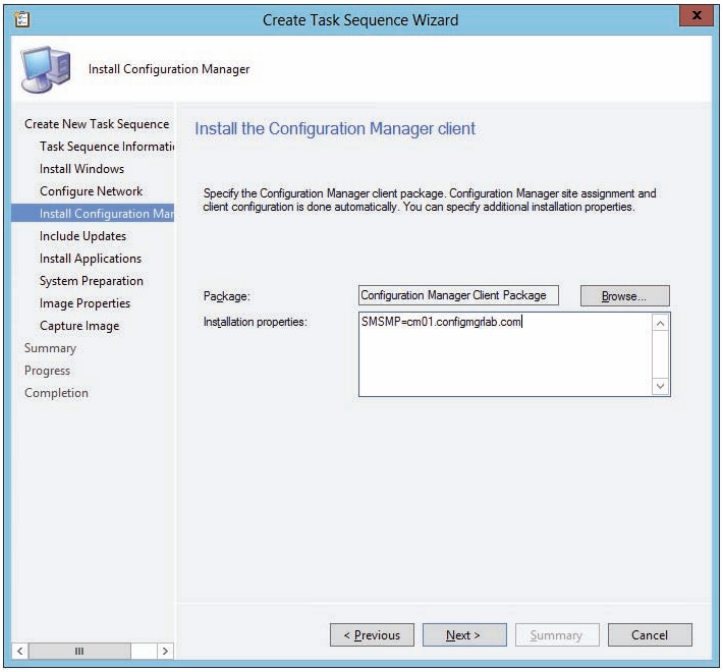


FIGURE 10.11
Install the Configuration Manager client task.

8. Select the Configuration Manager 2012 client package, and supply the `SMSMP=<siteservername>` installation properties, as shown in Figure 10.11.

   Supplying the installation properties allows you to install approved software updates via the Software Updates feature while the operating system is part of a workgroup.

9. Click Next.

10. Decide whether you want to install software updates during the build-and-capture process.

    Best practice is that you install all software updates that are approved in the Software Updates feature in Configuration Manager.

11. Click Next to be able to select the application that you want to install while building and capturing your reference operating system image, and click Next again.

12. Depending on the source of your operating system, you may need to supply a system preparation tool; click Next.

    When deploying Windows XP SP3, you need to use Sysprep to seal the operating system and make it anonymous before capturing. Windows 7, Windows Server 2008, and higher operating systems have a built-in system preparation tool.

13. Supply information about the image, such as creator, version, and description, and click Next.

14. Supply a UNC path and a filename for the captured operating system image, as shown in Figure 10.12, and click Next.

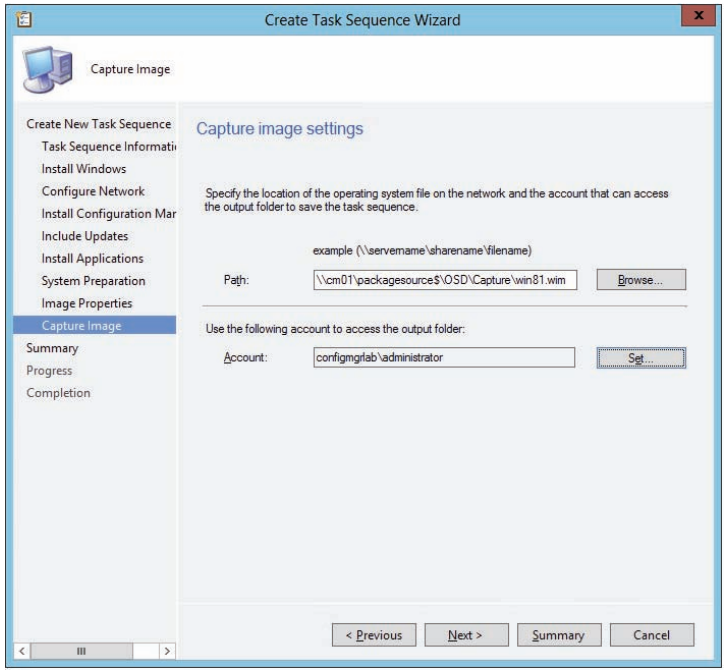


FIGURE 10.12 Captured image path and filename

15. Supply an account with Write permission to the share where the image will be captured. Click Test Connection if you want to test whether the user name and password are correct.
16. Click Next to see the summary.
17. After reviewing the summary, click Next to create the task sequence.
18. When finished, click Close.

As mentioned earlier, if you want to use the operating system installer image to build and capture the operating system image, you need to change the just-created build-and-capture task sequence. This is optional.

Optional:

1. Select the just-created task sequence and click Edit on the Home tab of the ribbon of the Configuration Manager console.
2. Select the Apply Operating System task, and click the Apply Operating System From An Original Installation Source radio button, as shown in Figure 10.13. Then click Browse to select Windows 8.1 Enterprise Operating System Install Package For This Task Sequence. Click OK to save the changes.

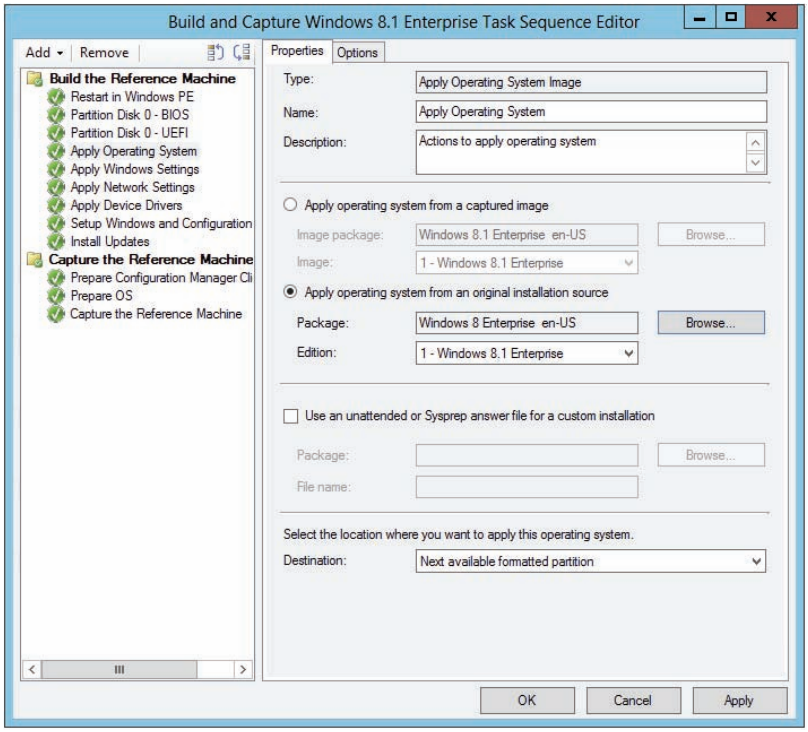


FIGURE 10.13
Apply Operating System task

Task Sequences Used with Media Boot

If you do not want to enable PXE support on your distribution points or you want to capture a custom reference computer, you can also create a build-and-capture task sequence that runs from media. Follow these steps to create a task sequence for creating a capture image:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. From the Home tab of the ribbon, click Create Task Sequence Media. This opens the Select Media Type page, shown in Figure 10.14.

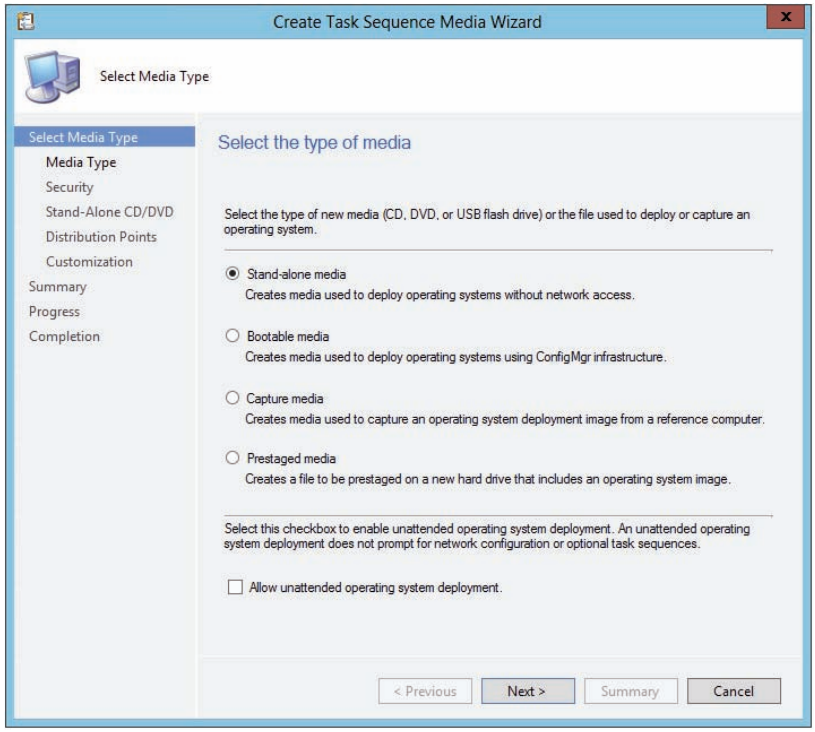


FIGURE 10.14 Create Task Sequence Media Wizard—Select Media Type page

3. On the Select Media Type page, select Capture Media, and then click Next.

   By selecting Capture Media, you will be creating the capture media that will be used to capture the operating system image.

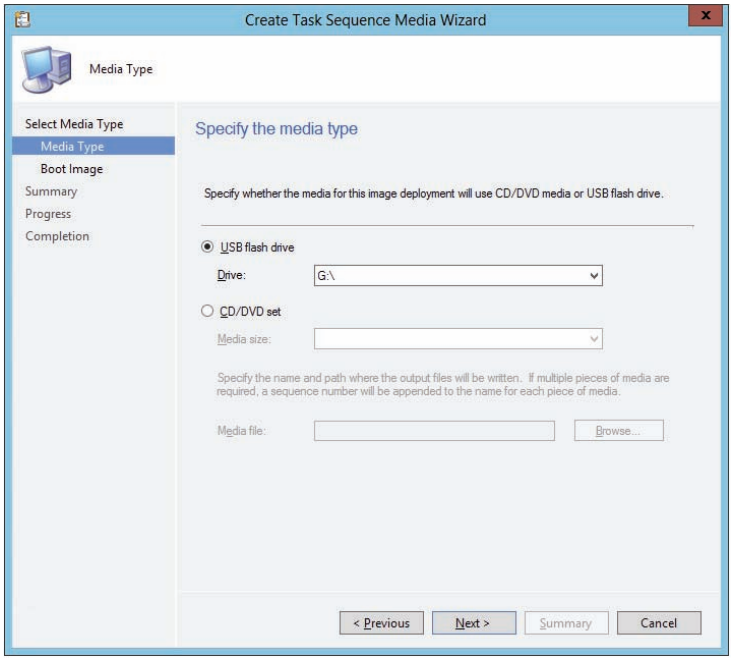


FIGURE 10.15
Create Task Sequence Media Wizard—Media Type page

On the wizard's Media Type page, shown in Figure 10.15, you can select the type of media to create.

4. For this example, select USB Flash Drive, select the available drive, and click Next. Click Yes at the dialog that warns you that the device will be formatted.
5. On the Boot Image page, shown in Figure 10.16, specify the boot image and distribution point you want to use. Click Browse, and select the boot image, and click Browse to select the distribution point. Click Next to continue.
6. Click Next on the Summary page, and Configuration Manager 2012 will begin creating the capture media on the USB stick.
7. Finally, you will be presented with the Wizard Completed page; click Close.

When finished, you can use the USB stick to boot up the computers that you will be using to build your operating system image. If you have selected to create an ISO file, you can now burn that ISO file to a CD and use that CD to boot up the computers in which you will be building your operating system image.

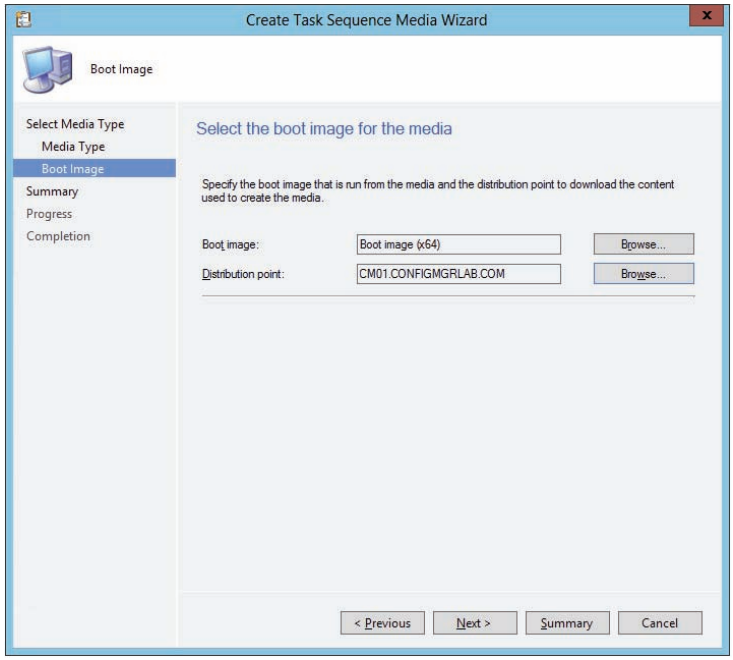


FIGURE 10.16
Create Task Sequence Media Wizard—Boot Image page

Capturing an Operating System Image

Configuration Manager 2012 supports two different ways of capturing an operating system image. You can use the fully automatic way, by using the build-and-capture task sequence, or you can capture a custom reference computer, by using the capture media created earlier.

Building and Capturing Automatically

When building and capturing an operating system image with the specially designed build-and-capture task sequence, you can fully automate the build-and-capture process. This way you know that the result of a task sequence is always the same, and no user intervention is necessary.

To be able to use the build-and-capture task sequence created earlier, you need to make the task sequence available for deployment, as follows:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Select the build-and-capture task sequence, and click Deploy on the Home tab of the ribbon.
3. Specify the collection where the reference computer resides, and select the distribution point(s) where the content needs to be deployed to, as shown in Figure 10.17.

   Be sure that you create a special collection for building and capturing operating systems.
4. Click Next to proceed in the wizard.

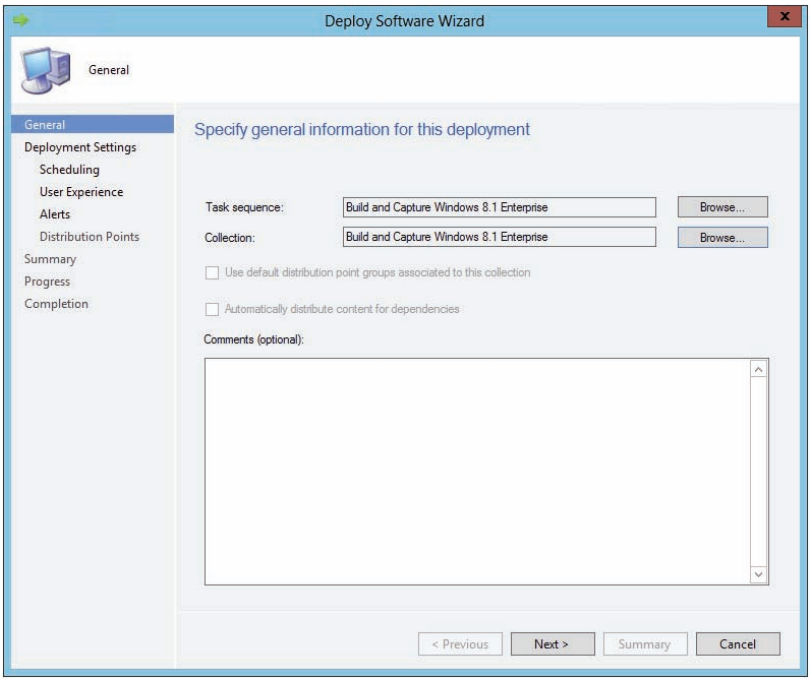


FIGURE 10.17
Specify deployment information

Now you need to configure the deployment settings; for Purpose you can select either Available or Required. If you choose Available, you need to press F12 to enter the PXE boot procedure and select the task sequence in the WinPE environment. If you choose Required, the machine will boot into WinPE during the PXE boot procedure. You also need to configure in which scenario the deployment is available.

Only Configuration Manager Clients A task sequence deployment can be made available for Configuration Manager clients only. This means that an operating system with a Configuration Manager client must be active to be able to receive and start the task sequence deployment. This option can be used best in refresh client scenarios.

Configuration Manager Clients, Media And PXE If the task sequence that needs to be deployed must be available in all scenarios, you need to select this option.

Only Media And PXE When a task sequence like the build and capture one needs to be available only for media and PXE, then you need to select this option. Another scenario is bare-metal deployment.

Only Media And PXE (Hidden) When a task sequence like the build and capture one needs to be available only for media and PXE, then you need to select this option. Another scenario is bare-metal deployment. This is often used for test purposes. To be able to use the hidden deployment, you need to set the `SMSTSPreferredAdvertID` variable with the `AdvertID` of the Task Sequence as the value at the collection level where the task sequence is deployed.

Click Next.

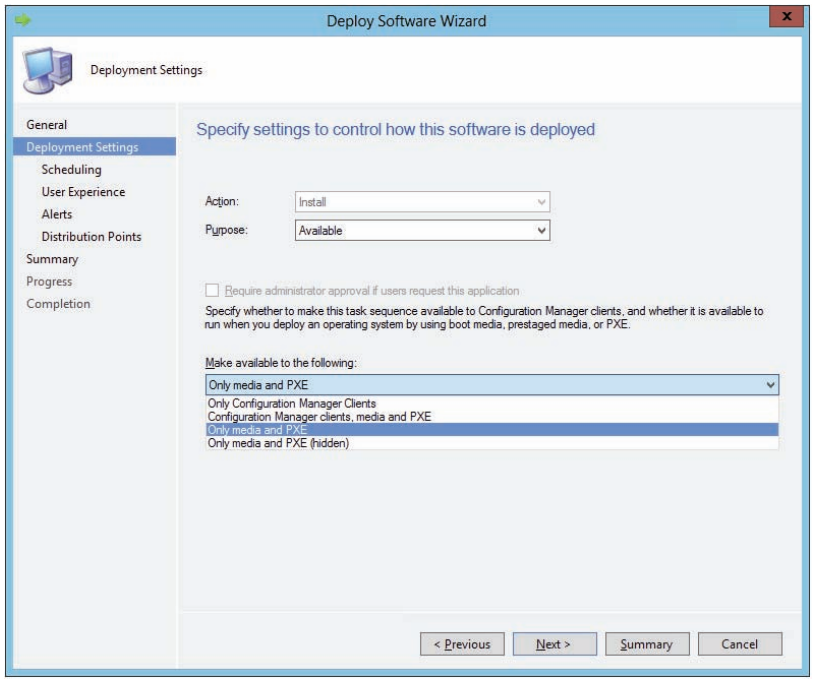


FIGURE 10.18 Specify the deployment settings.

5. Select the option Only Media And PXE, as shown in Figure 10.18, and click Next to configure the deployment settings.
6. Configure the scheduling settings, and click Next.
7. Since you are configuring a deployment for a build-and-capture task sequence, no user experience options need to be configured, so click Next.
8. Configure Alerts options for failed deployments; you can set a threshold for alerts to be sent when the threshold is higher than a percentage of failed deployments. Click Next to proceed.
9. Configure the distribution point settings, and click Next to review the summary.
10. After reviewing the summary, click Next and then Close.

After making the build-and-capture task sequence available for deployment, you can go into action and build and capture the image. To begin, shut down your reference computer and be sure that you can boot from the network. To cause less overhead on drivers, building and capturing images is often done with virtual machines. To use the following procedure, be sure that your computer object in Configuration Manager is added to the collection where the task sequence is deployed.

1. Start your computer or virtual machine and boot into PXE.
2. At the Welcome To This Task Sequence screen, click Next.
3. Select the Build And Capture Windows 8.1 Enterprise task sequence, as shown in Figure 10.19, and click Next.

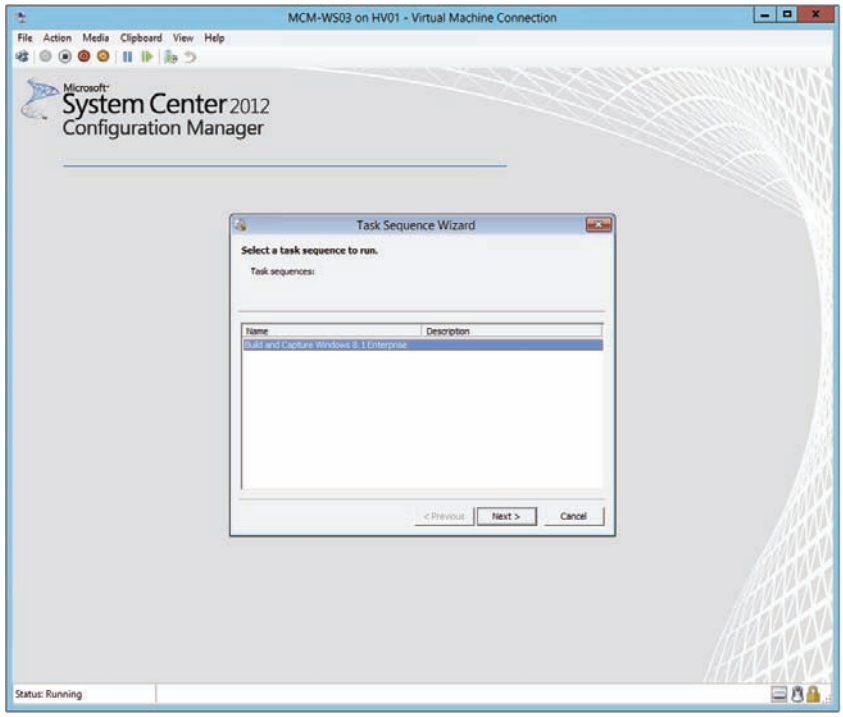


FIGURE 10.19
Select the task sequence

After the build-and-capture process, described earlier, has finished, you will have your captured Windows image. The computer will restart in Windows.

The captured WIM image can be used for deployment to the computers in your environment. Be sure to always test your deployment in a test environment.

Capturing a Reference Computer

When creating an image of a reference computer, you need to be aware of a few issues. First, ensure that the computer is a member of a workgroup instead of a member of the domain. This is a required step; if the reference computer is a member of the domain, you will be required to remove it from the domain to create the image of the operating system of the computer. Second, we recommend removing the Configuration Manager client from the machine. This is not a requirement, just a recommendation.

1. To begin creating an image of the reference computer, insert the CD that was created from the ISO file you created earlier.
2. Run `LaunchMedia.cmd` located in the root folder on the CD. This opens the Image Capture Wizard.

3. Click Next to open the Image Destination page, shown in Figure 10.20, which allows you to specify where to copy the image when the capture is completed.

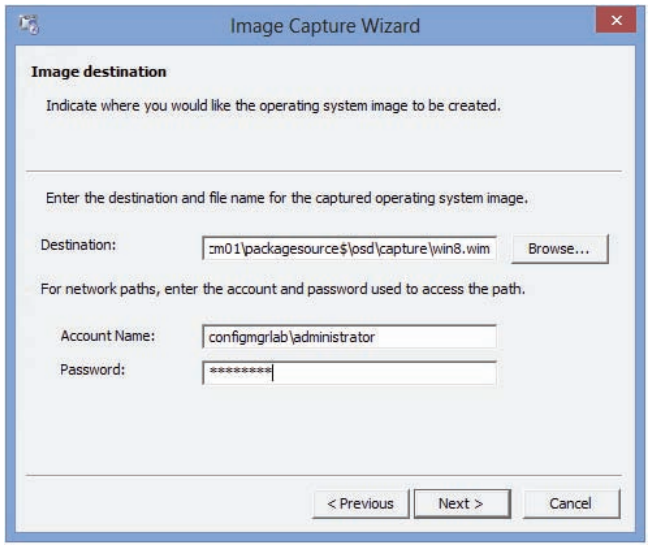


FIGURE 10.20
Image Capture Wizard—Image Destination page

4. Fill in the correct information, and click Next.

   As you can see, we copy the WIM file to our site server.

   You will now be able to add some information about the image on the Image Information page. You can fill in the Created By, Version, and Description fields for the WIM file.

5. Fill in this information with as much detail as you can; then click Next.

6. On the Summary page, click Finish to begin the capture phase.

   An Installation Progress window appears, telling you that the Image Capture Wizard is working and running in the background. When the image capture is complete, a System Restart message will appear, and the system will reboot. When the system reboots, it will boot into WinPE and begin capturing the system. This process can be a lengthy one, so be patient while the operating system is being captured.

   Once the image capture is complete, you will see the Image Capture Wizard success message, shown in Figure 10.21.

7. Click OK to allow the machine to reboot and return to the operating system.

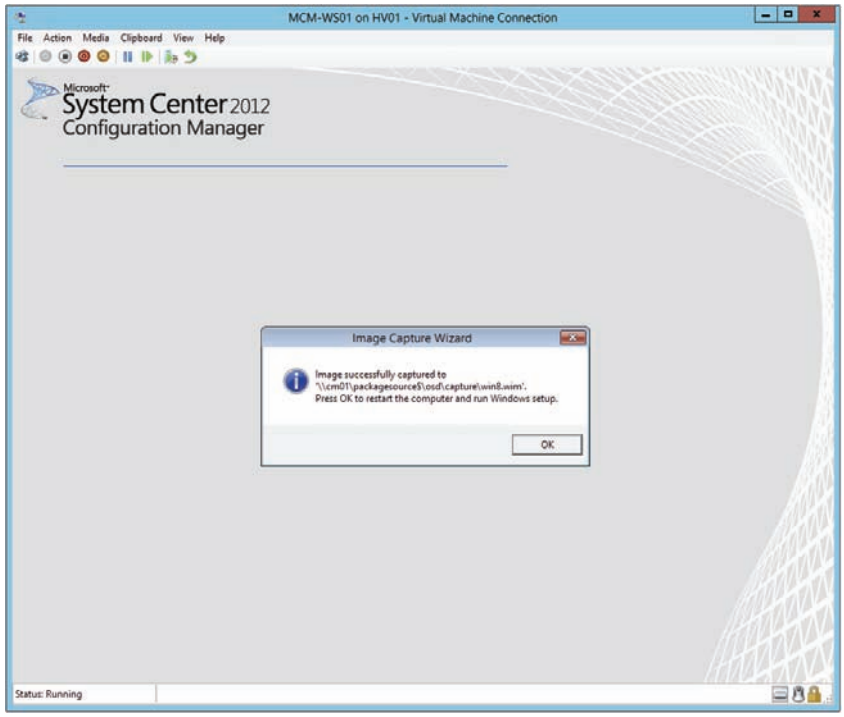


FIGURE 10.21 Image capture success message

Deploying an Image

Since you've now successfully captured an image, you need to add this operating system image to Configuration Manager. Then you need to deploy this image by creating a task sequence and deploy this task sequence to the computers in your environment. Always be sure to thoroughly test the image in a separate test environment before deploying it into production.

Adding a Captured Image

The WIM file that you just created needs to be added as an available operating system for Configuration Manager 2012. To deploy this image, follow this procedure:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Images.
2. Click Add Operating System Image on the Home tab of the ribbon.

   This opens the Add Operating System Image Wizard's Data Source page.
3. Ensure that the (UNC) Path field points to the location where the WIM file was created, and click Next.

The General page allows you to customize the Name, Version, and Comments fields for the image file.

4. Fill in the appropriate information, and click Next.
5. The Summary page will be displayed; review the information and click Next.
6. Finally the Wizard Completed screen will appear. On this page, click Close.

Distributing and Deploying the Image

Next, you need to configure a distribution point in order to distribute this image. This step is a little different from the steps for assigning distribution points for packages that we discussed elsewhere in this book:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Images.
2. Select the image that you added, and click Distribute Content on the Home tab of the ribbon.
3. In the Distribute Content Wizard click Next.
4. Click Add and select Distribution Point or Distribution Point Group.
5. Select in the Add Distribution Points or Add Distribution Point Groups dialog the distribution points or groups that you want to distribute the WIM image to, and click OK.
6. Click Next to review the summary.
7. After reviewing the summary, click Next and then Close.

Developing a Task Sequence for Deployment

Now you will need to create a task sequence for deploying the Windows operating system image. Creating a task sequence will give Configuration Manager 2012 a series of steps to perform on the new installation of the workstation:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Select Create Task Sequence on the Home tab of the ribbon.

   This will open the New Task Sequence Wizard's Create A New Task Sequence page.
3. Because you have already built an image of a Windows client, select Install an existing image package, and then click Next.

   This opens the New Task Sequence Wizard's Task Sequence Information page.
4. Specify the task sequence name and a comment, and specify the boot image to use during the installation of the image. Click Next after supplying the information.

   The Install Windows page, shown in Figure 10.22, allows you to specify the Configuration Manager 2012 image package containing the operating system you want to install.

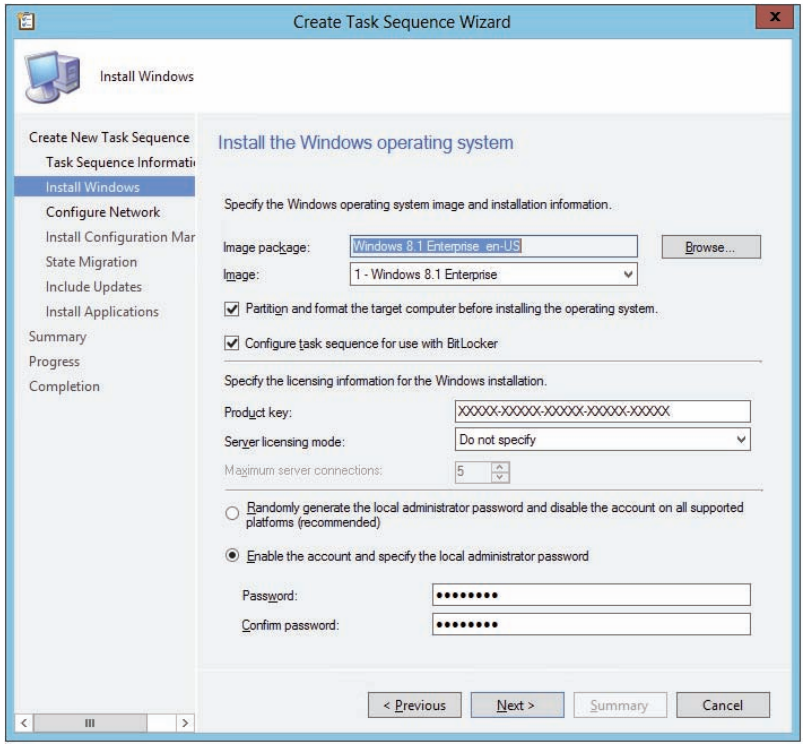


FIGURE 10.22 Create Task Sequence Wizard—Install Windows page

5. Click the Browse button to find the image of the operating system you want to install, and click OK.
6. If you want to partition and format the target computer before installing the operating system, leave the Partition box selected, and format the target computer before installing the operating system.
7. Keep the Configure Task Sequence For Use With BitLocker option enabled if you want to enable BitLocker during the deployment of the Windows image.
8. Enter the licensing information for the version of Windows you are installing in the Product Key field, and click Next.
9. On the Configure Network page, select the domain or workgroup to join.

   If you select to join a domain, you can specify which OU to put the computer in once it joins the domain. If you select to join a domain, you will need to specify the account that has permission to join computers to a domain. The Configuration Manager Network Access Account is often used to join the computer to the domain. You need to delegate this access to the user account. Verify the account by testing the connection after configuring the account.

10. Click Next to continue.

    Now all the work you did earlier will finally be put to use.

11. On the Install Configuration Manager Client page, specify any additional installation properties. Click Browse if you do not want to use the default Configuration Manager 2012 client package.

12. Then click Next to continue.

    The Create Task Sequence Wizard page that appears is State Migration, shown in Figure 10.23, which allows you to configure the user state migration capture.

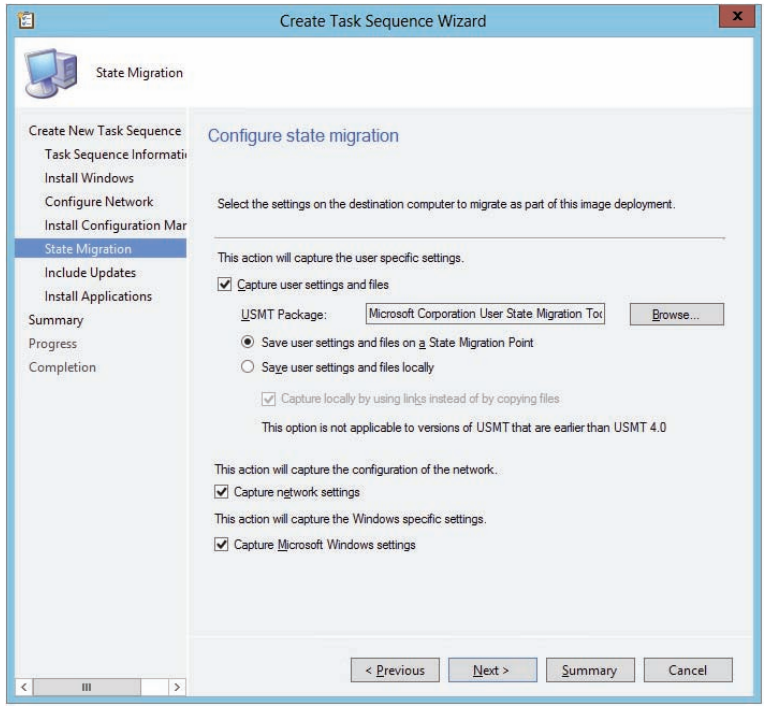


FIGURE 10.23
Create Task Sequence Wizard—State Migration page

13. Select or deselect whether you want to capture network and Microsoft Windows settings.

14. Click Browse, if you do not want to use the default User State Migration Tool package, and then click Next.

    After you've configured the state migration, the Include Updates page will appear, which allows you to specify whether the client will get mandatory, all, or no software updates after the image has been installed.

15. Configure the installation of software updates, and click Next.

    Now you have the option to install additional applications by adding the configured applications to the task sequence. This is extremely useful if you have a large number of applications you want installed on each system after the operating system has been installed. Figure 10.24 shows the Install Applications page, where you can specify the additional applications.

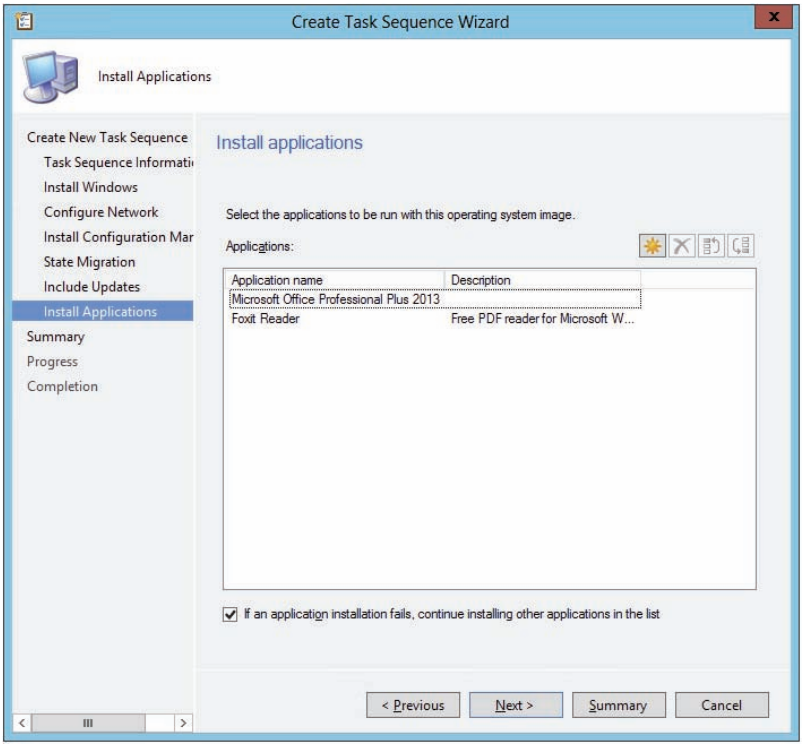


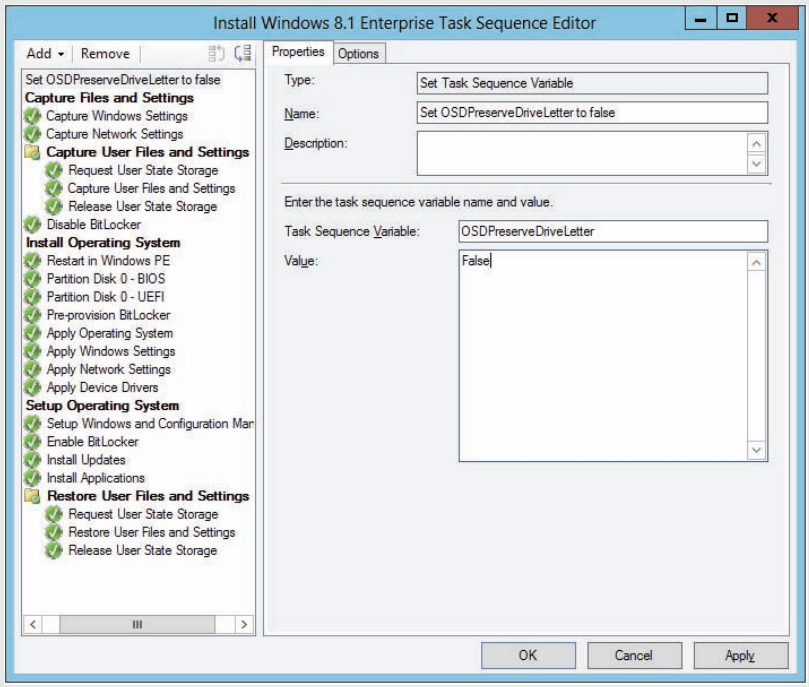
FIGURE 10.24 Create Task Sequence Wizard—Install Applications page

16. Select the option If An Application Installation Fails, Continue Installing Other Applications In The List if you want to let the task sequence proceed with its tasks.
17. Click Next once you have the additional applications specified.
18. Click Next on the Summary page, and Configuration Manager 2012 will complete the Create Task Sequence Wizard.
19. Click Close.

Preserve the Drive Letter in Your Image, or Not

A disadvantage of deploying the default `INSTALL.WIM` files is that Microsoft created the `INSTALL.WIM` image by installing the Windows 7 version to the D: drive. For this reason the Windows operating system is installed by default to the D: drive.

You can disable this default behavior by setting a task sequence variable at the top of the task sequence.



Adding the task sequence variable `OSDPreserveDriveLetter = False` to the task sequence allows you to install the default `INSTALL.WIM` image to drive C: instead of drive D:.

Deploying the Task Sequence

You have successfully created a new task sequence to install a new operating system on a machine, join the system to the domain, and install the Configuration Manager 2012 client on the machine once it comes online. However, the task sequence won't do you any good unless you deploy it to a collection. Take the following steps to do so:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Select the task sequence you want to deploy, and click Deploy on the Home tab of the ribbon.
3. Click Deploy to open the General page of the Deploy Software Wizard.

4. Click Browse to find the collection where you want to install this operating system package, and then click Next to continue.

   The next wizard page is Deployment Settings, shown in Figure 10.25.

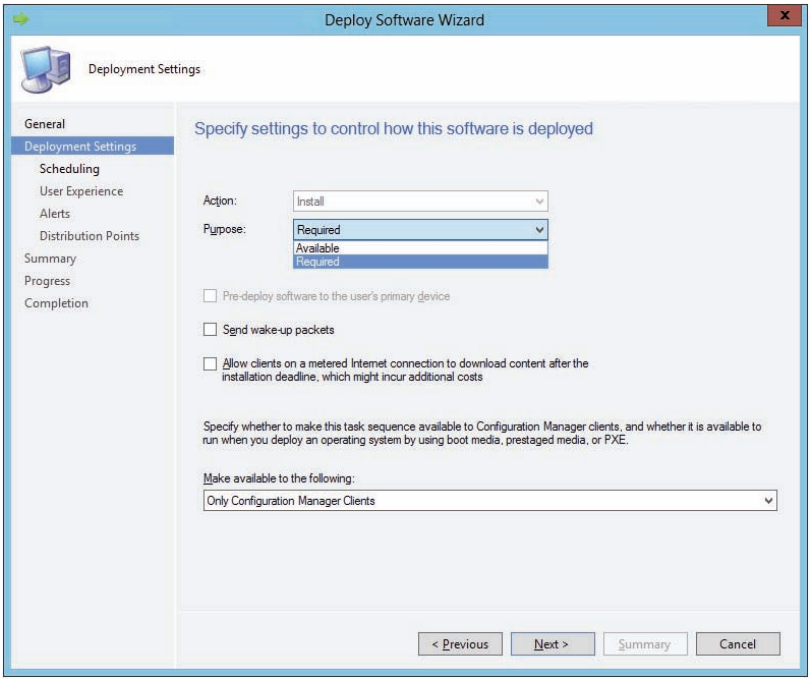


FIGURE 10.25 Deploy Software Wizard—Deployment Settings page

5. Supply the purpose of the deployment.

   - If you want to let your users choose to reinstall their operating system, choose the Available option.
   - If you want the installation to start automatically, choose the Required option.

   Choosing the Required option enables you to send wake-up packets to the computers in the collection. Of course, you need to first configure Wake On LAN support in Configuration Manager 2012. At this time you do not need to enable the option for PXE support; the task sequence you are creating is used to refresh your Windows installation, so you will be making the deployment available only for Configuration Manager clients.

6. Click Next to continue.

   The next step is to configure the scheduling options for the deployment.

7. Configure the availability of the deployment and when the deployment will expire.

8. Define the assignment schedule, and be sure to set the rerun behavior to Rerun if the previous attempt failed.

If you do not set this option, the deployment will rerun as soon the deployment is finished, thereby creating a deployment loop.

9. Click Next to proceed.
10. On the User Experience page, specify how users are notified about the deployment and how they interact with the deployment.

    We prefer to show the task sequence progress to let the end user know that the computer is being reloaded.

11. Click Next to proceed, and configure the Alerts options for this deployment.
12. Click Next, configure how to run the content for this deployment on the Distribution Points page, and click Next again.
13. Review the summary, click Next, and click Close when the wizard has finished processing the deployment.

Now you have created the deployment for the operating system deployment, and any system in the collection you specified will get the new deployment during the next policy refresh. Once the policy refresh takes place, the workstation will receive the Assigned Program About To Run notification. Once the installation begins, you will see the Installation Progress message box in Windows, as shown in Figure 10.26.

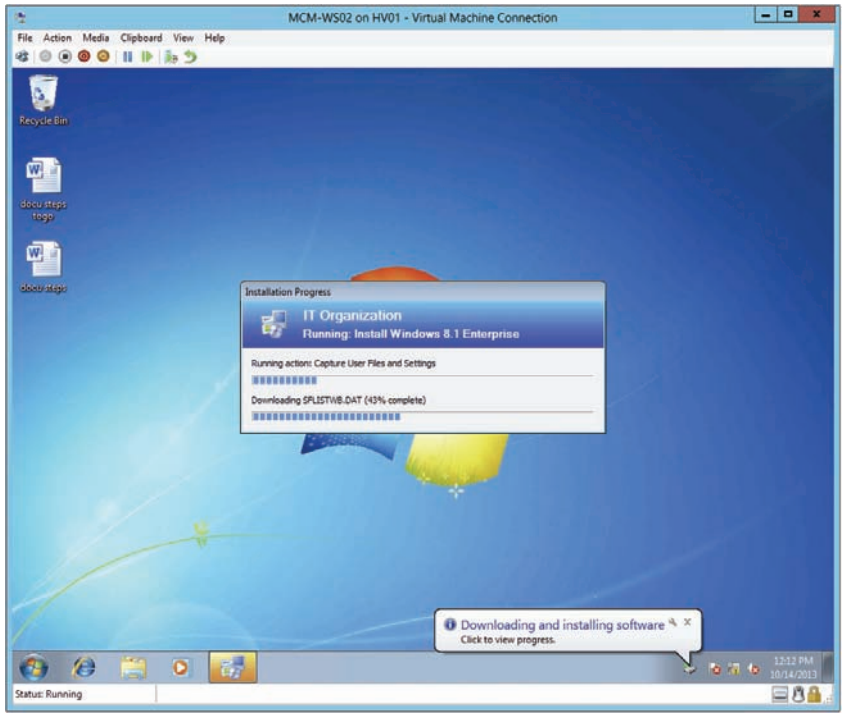


FIGURE 10.26 Installation Progress message box

The system will automatically reboot and then begin the boot to WinPE, as shown in Figure 10.27.

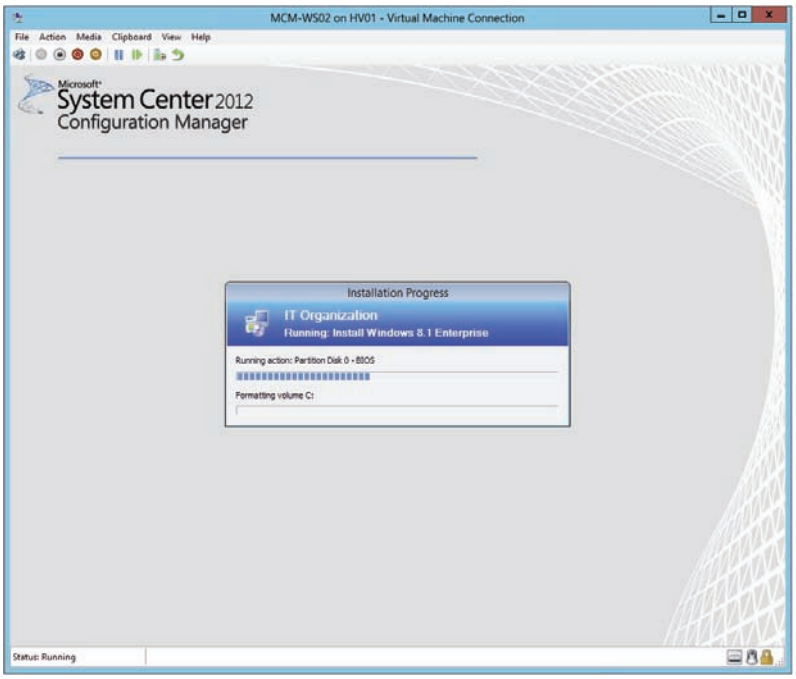


FIGURE 10.27
Booting to WinPE

The installation will take some time to complete. During this install, Configuration Manager is gathering the user state and saving the date in the USMT folder on the site server, which you configured earlier in this chapter. You can monitor the `<drive>:\USMTData` folder on the site server to see the user state migration data being copied to the server.

Configuration Manager will push the new operating system down to the new machine and then join it to the domain, install the Configuration Manager client, and finally copy back all the user data on the client.

You can monitor the progress of the operating system deployment in the Deployment Status window, shown in Figure 10.28.

1. From within the Configuration Manager console, choose the Monitoring workspace, expand Overview ➢ Deployments, and select the deployment that you want to monitor.
2. After selecting the deployment, click Run Summarization on the Home tab of the ribbon.
3. After the summarization is updated, click View Status on the Home tab of the ribbon to see the status of the deployment, as shown in Figure 10.28.
4. While viewing the status, you can refresh the status by clicking Run Summarization or Refresh.

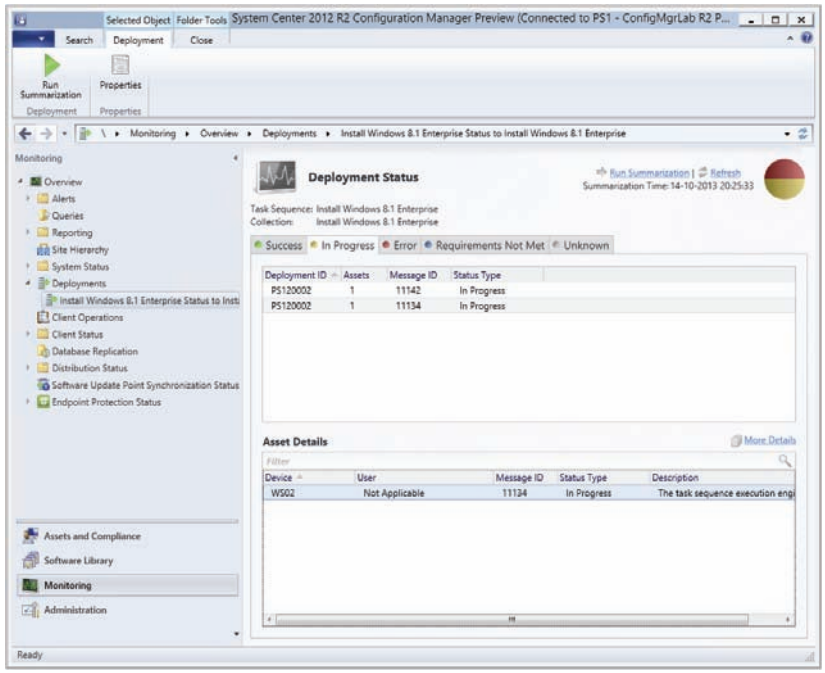


FIGURE 10.28
Monitoring the OSD deployment status

5. While monitoring the OSD deployment status, you are able to review the completed tasks by selecting More Details and selecting the Status tab of the Asset Message dialog screen, as shown in Figure 10.29.

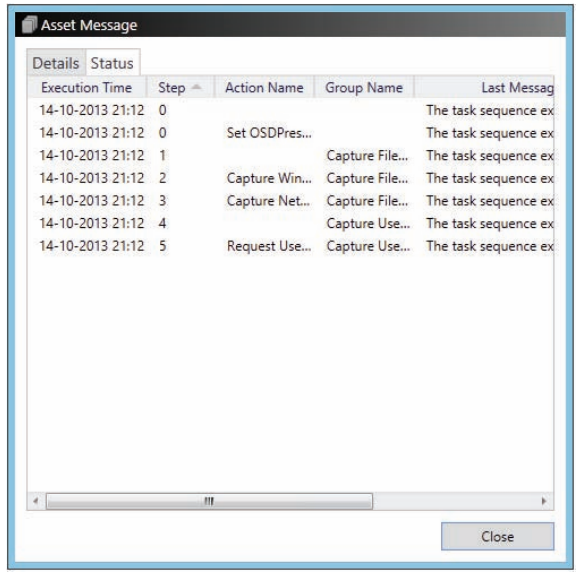


FIGURE 10.29
Review the task sequence steps in the Asset Message dialog screen.

Deploying the Operating System on Bare Metal

After deploying an operating system in a refresh scenario, you also need to create a task sequence and deployment to be able to deploy an operating system to bare-metal computers. *Bare-metal* computers are computers without any operating system present.

To deploy an operating system to a bare-metal computer, you can use a CD or DVD to start into WinPE, but you can also boot into PXE to start the WinPE image from the network. Let's see how this works with PXE. To be able to deploy an operating system to a bare-metal computer, you need to perform the following tasks:

- Import information about a computer.
- Create a task sequence.
- Deploy the task sequence.

Importing Computer Information

Now you are ready to set up a computer association so that Configuration Manager can identify the bare-metal machines that will receive a fresh install. To specify the computer association, you will need to open the Configuration Manager console and proceed as follows:

1. From within the Configuration Manager console, choose the Assets And Compliance workspace and expand Overview ➢ Devices.
2. Click Import Computer Information on the Home tab of the ribbon.

   This will allow you to import a single computer or import many systems from a comma-separated values (CSV) file.
3. Select the option Import Single Computer, and click Next.

   This will bring up the Single Computer page, as shown in Figure 10.30.

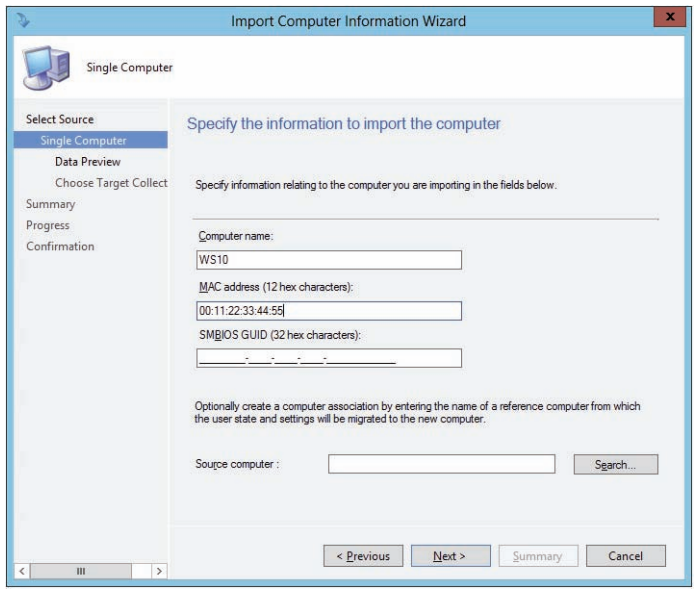


FIGURE 10.30 Import Computer Information Wizard—Single Computer page

You must enter the computer name along with either the MAC address or the SMBIOS GUID. The computer name is just how the machine will appear in the collections, not what the actual computer will be named.

4. Fill in the appropriate information, and then click Next.
5. This sends you to the Data Preview page; check the information and click Next.

   You'll then see the Choose Target Collection page.
6. Here, specify which collection you want to add to this new machine.

   It is extremely important to put all the bare-metal installs into the same collection, used only for bare-metal deployment.
7. Click Next.
8. After specifying the collection, you will see the Summary page. Click Next, and then click Close on the Finish page.

Creating a Task Sequence for the Bare-Metal OSD

When you deploy a bare-metal machine, it is wise to create a dedicated task sequence for this purpose. Once you create this special task sequence, you need to deploy it to a special collection in which you can place the bare-metal computers.

Creating a task sequence for deploying an image to a new machine is very straightforward:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. From there, click New Task Sequence on the Home tab of the ribbon of the Configuration Manager console.

   This opens the Create New Task Sequence page of the New Task Sequence Wizard.
3. Select the Install An Existing Image Package option, and click Next.
4. On the Task Sequence Information page, fill in the name, optionally add a comment, and select the boot image you want to use for the operating system deployment and click Next.
5. On the Install The Windows Operating System page, select the image package by browsing to the correct image.
6. Because this example is deploying Windows to a bare-metal machine, enable the option to partition and format the target computer.

   The next options you can configure are the network settings.
7. On the Configure The Network page, specify whether you want to join the new machine to the domain or join a workgroup. Click Next after configuring the network settings.

   A Configuration Manager task sequence will allow you to install the Configuration Manager client during an operating system deployment.

8. On the Install The Configuration Manager Client page, add installation properties if you need to and click Next.
9. Since you are deploying Windows to a bare-metal machine, on the State Migration page, shown in Figure 10.31, deselect all the options because you do not need to worry about capturing any data from these machines. Click Next to configure the installation of software updates.

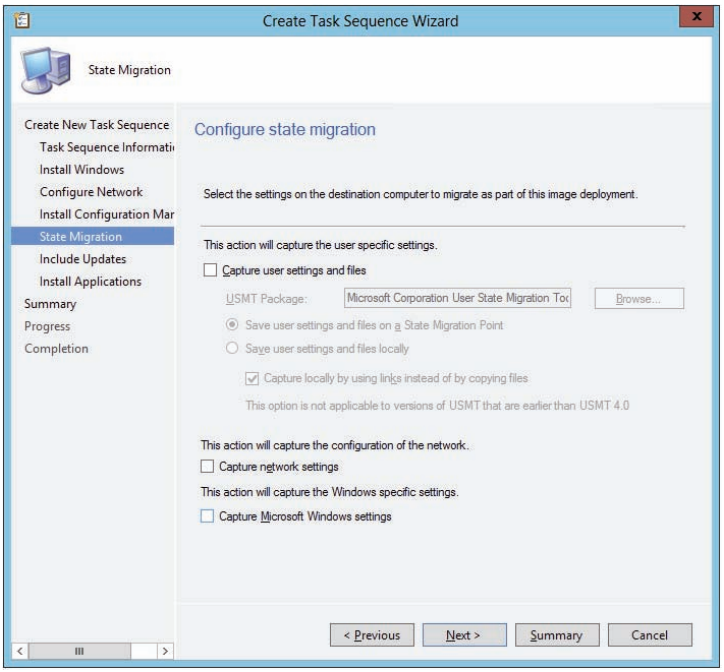


FIGURE 10.31 Create Task Sequence Wizard—State Migration page

On the Include Updates page, you can now allow Configuration Manager to include software updates during the install.

10. Make the selections you desire, and click Next.

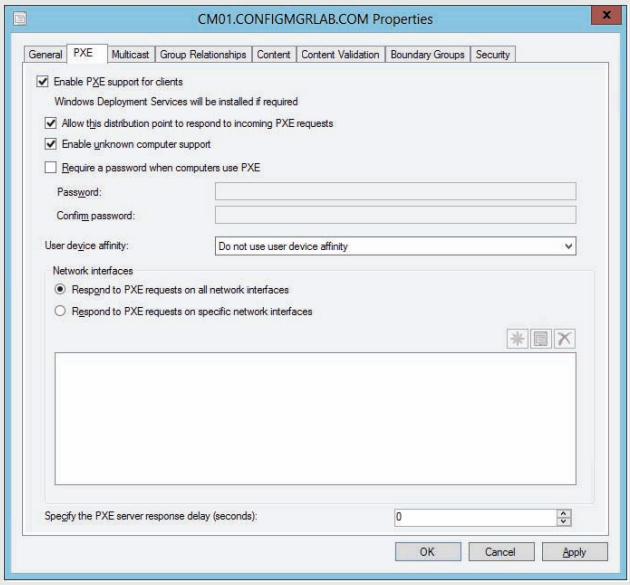
    If you have any additional applications you want to deploy, such as Microsoft Office or anything else, on the Install Applications page, you can add any applications to install on the machine after the operating system has been deployed.
11. Click Next to view the Summary page.
12. After viewing the summary, click Next and then Close to complete the wizard.

Deploying the Bare-Metal Task Sequence

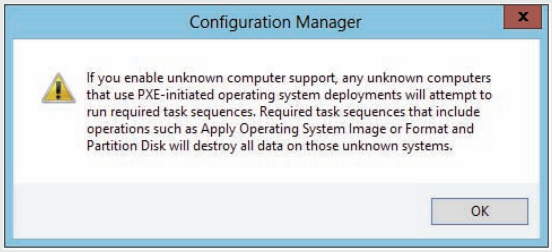
After creating the task sequence for bare-metal deployment, you need to deploy this task sequence, as discussed earlier. Be sure to select that the task sequence is available to only media and PXE.

Using the Unknown Computer Collection

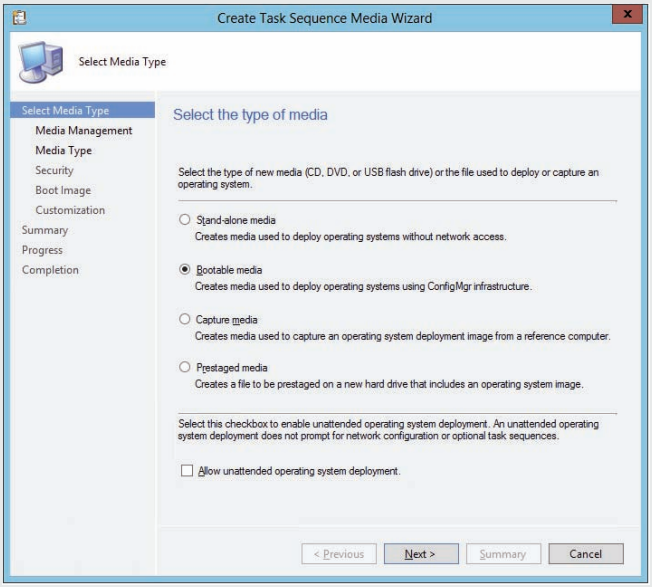
You can enable support for unknown computers. Unknown computer support is a feature in Configuration Manager 2012 that will allow unmanaged systems to be managed with Configuration Manager 2012 during an OS deployment. To do so, open the Configuration Manager console, select the Administration workspace, and expand Overview ➢ Site Configuration ➢ Servers And Site System Roles. Select the server with the distribution point where PXE is enabled, and click Role Properties in the Site Role section of the ribbon. Browse to the PXE tab in the Distribution Point Properties dialog box, shown here, and select the box Enable Unknown Computer Support.



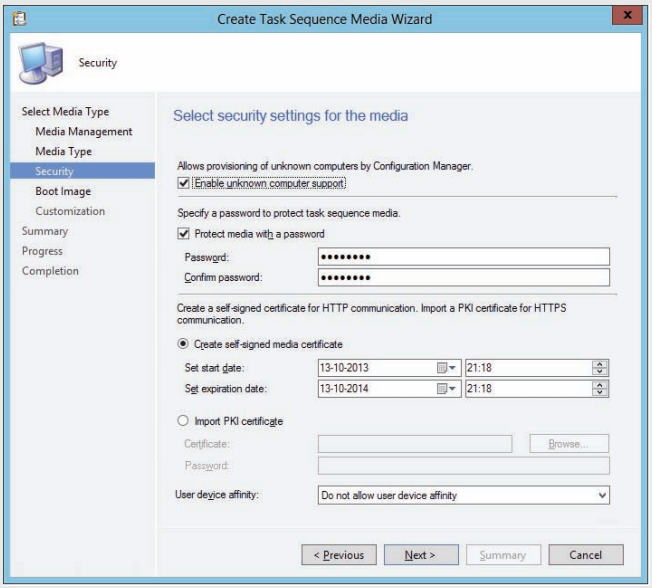
When you enable this option, you will be prompted with the caution message shown next. Assuming you are ready to proceed, click OK.



To create a task sequence for bootable media, open the Configuration Manager console, choose the Software Library workspace, and expand Overview ➢ Operating System ➢ Task Sequences. Click Create Task Sequence Media on the Home tab of the ribbon. This opens the Create Task Sequence Media Wizard's Select Media Type page.



Select Bootable Media, and click Next. Choose Dynamic Media when the media contacts a management point, which redirects the client to a different management point based on the client location in the site boundaries, or choose Site-Based Media when you want to specify a management point. Click Next to configure the media type. On the Media Type page, select the type of media you will be using, either a USB flash drive or a CD/DVD set, and then click Next. The Security page offers the Enable Unknown Computer Support option. Selecting this will allow you to target the unknown computer collection with the operating system deployment.



The next step, after configuring unknown computer support, is configuring the boot image, distribution point, associated management points, and customizations.

After creating the boot media you can create a deployment to this collection for the OSD task sequence, and Configuration Manager will process the task sequence for the unknown computers. Be sure to enable your deployment to be accessible for boot media and PXE.

Installing Device Drivers into OSD

Now you have configured one package to perform Windows upgrades and another package to install that same Windows install package onto a bare-metal system. But what happens if you get a new system with a completely new setup, including device drivers that are not installed within the current package, so that when the machine comes online it will not be able to attach to the network?

Microsoft has provided the ability to import device drivers into Configuration Manager 2012 and add them to the boot images or driver packages so they can be installed as part of the operating system deployment task. To import Windows device drivers, take the following steps:

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Drivers.
2. Click Import Driver on the Home tab of the ribbon of the Configuration Manager console.

   This opens the Locate Driver page, shown in Figure 10.32.

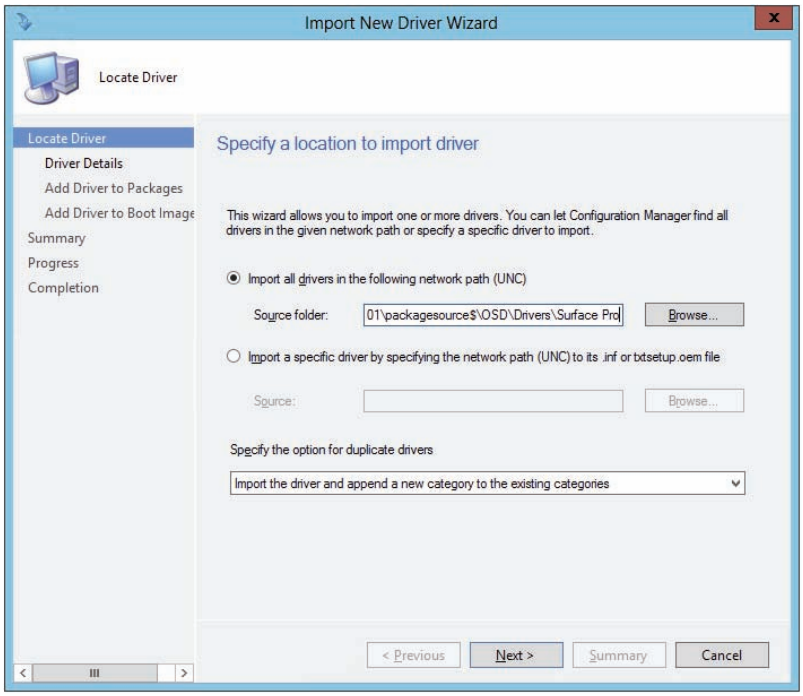


FIGURE 10.32 Import New Driver Wizard—Locate Driver page

3. You can specify to import all drivers or just a single device driver. When importing drivers you could run into the fact that there are duplicate drivers. Next, you should configure the import behavior when duplicate drivers are detected; you can configure the following options:
   - Import the driver and append a new category to the existing categories.
   - Import the driver and keep the existing categories.
   - Import the driver and overwrite the existing categories.
   - Do not import the driver.
4. Click Next after picking the correct driver(s), and then you will be presented with the Driver Details page. Next you should assign the driver(s) to one or more categories.

Working with Categories Enables You to Manage Drivers

If you add categories to drivers, you can manage your drivers in the store more easily. By adding the category to the search criteria, you can easily select the drivers and delete them by clicking Delete on the Home tab of the ribbon in the Configuration Manager console.

5. On the Add Driver To Packages page, shown in Figure 10.33, specify the package(s) you want to add this driver to, or specify a new package. If you need to create a new driver package, do the following.

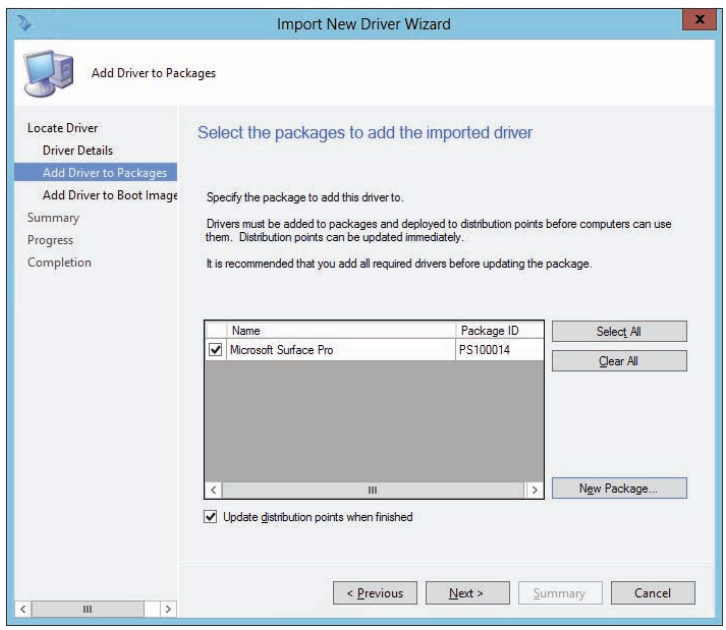


Figure 10.33 Import New Driver Wizard—Add Driver To Packages page

a. Click New Package.

b. Supply a name and a UNC path for the source of the package.

c. Click OK.

d. If desired, select Update Distribution Points When Finished so the driver will be available as soon as possible to your site.

6. Click Next to continue.

7. Next, select which boot images you want to add the driver to, as shown in Figure 10.34. When selecting drivers in bulk—for instance, all drivers from one model—do not add these to the boot images. Add them in a later stage. It is a best practice to add only the missing NIC drivers and drivers related to storage (controllers) to the boot images.

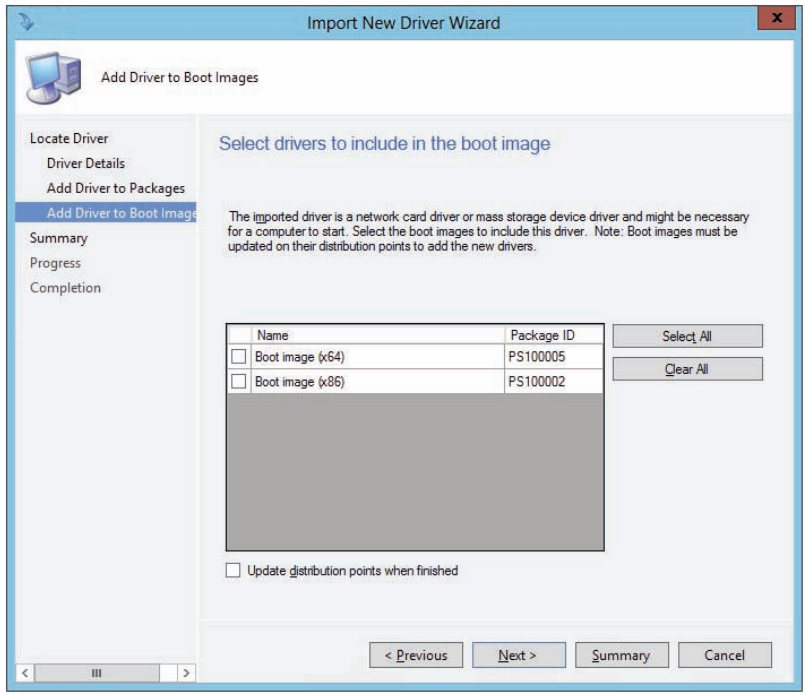


FIGURE 10.34
Adding drivers to boot images

8. Click Next to open the Summary page. Review the configuration, click Next, and then click Close.

Now Configuration Manager will inject that driver package into the packages and boot images you selected. This could take some time to process.

Using User Device Affinity

As discussed earlier, user device affinity enables you to deploy user-targeted applications during the operating system deployment process. There are several ways to configure user device affinity. Let's look at the following options:

- Manually configure a primary user for a device.
- Manually configure a primary device for a user.
- Configure a site to automatically create user device affinities.
- Import user device affinities.
- Enable users to configure their primary device.

Manually Configure a Primary User for a Device

To manually configure a primary user for a device, follow this procedure:

1. From within the Configuration Manager console, choose the Assets and Compliance workspace, expand Overview, and select Devices.
2. Select a device, and click Edit Primary Users on the Home tab of the ribbon. Search for the user, as shown in Figure 10.35, select the user, and click Add and then OK to set the primary user for the device.

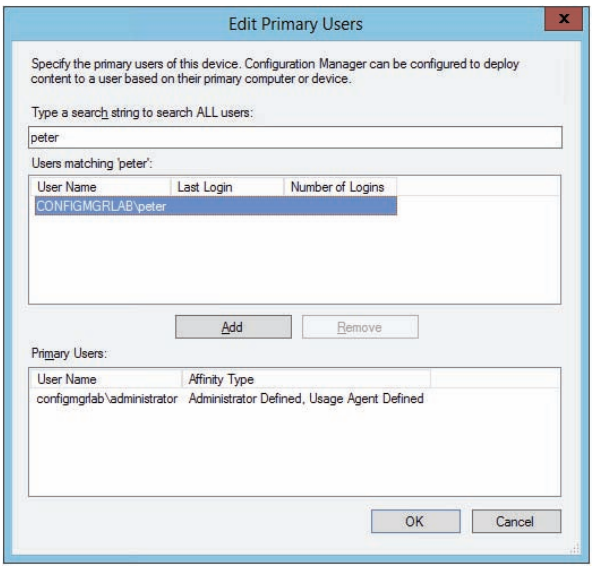


FIGURE 10.35 Search for and select the primary user

Manually Configure a Primary Device for a User

To manually configure a primary device for a user, follow these steps:

1. From within the Configuration Manager console, select the Assets And Compliance workspace, expand Overview, and select Users.
2. Select a user, and click Edit Primary Devices on the Home tab of the ribbon. Search for the device, select the device, and click Add and then OK to set the primary device for the user.

Configure a Site to Automatically Create User Device Affinities

With Configuration Manager 2012 you can also create the user device affinity automatically. Creating the affinity automatically is based on thresholds configured in the client settings. Configuring the client settings to create user device affinities is described here:

1. From within the Configuration Manager console, choose the Administration workspace, expand Overview, and select Client Settings.
2. Select the default client settings package or create a new client device agent settings package, and click Properties on the Home tab of the ribbon.
3. Select User And Device Affinity, as shown in Figure 10.36, and configure the following options.

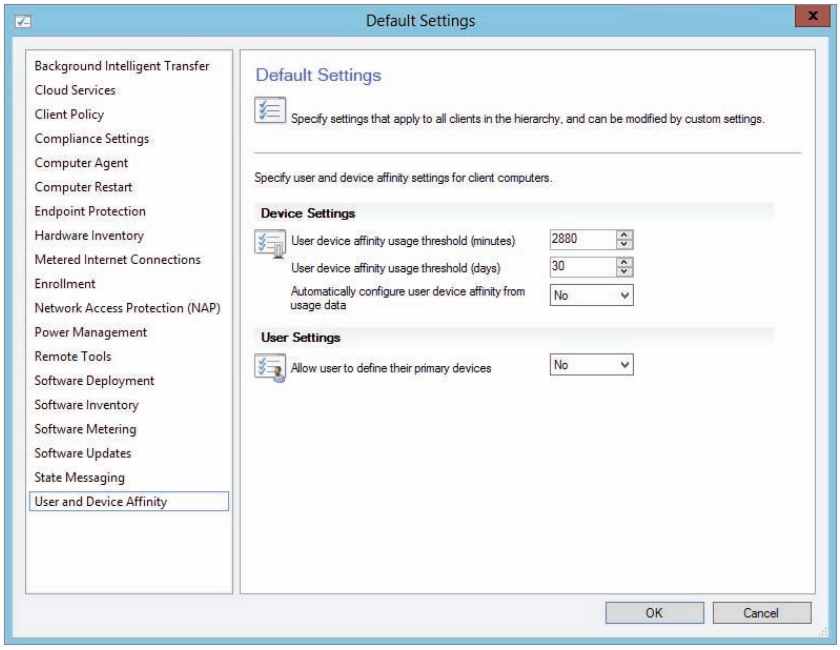


FIGURE 10.36
Configure client device settings.

User Device Affinity Usage Threshold (Minutes) Configure the number of minutes of usage by a user before a user device affinity is created.

User Device Affinity Usage Threshold (Days) Configure the number of days Configuration Manager will measure the usage of the device. For example, if User Device Affinity Usage Threshold (Minutes) is configured with a value of 120 minutes and User Device Affinity Usage Threshold (Days) is set to 14 days, the user must use the device for 120 minutes over a period of 14 days before the user device affinity is created.

Automatically Configure User Device Affinity From Usage Data Enable the feature by setting the value to Yes, or disable the feature by setting the value to No.

Import User Device Affinities

If you have the information from your client computers and primary users in a CSV file, you can import the user device affinity information to Configuration Manager 2012.

1. From within the Configuration Manager console, select the Assets And Compliance workspace, expand Overview, and select Devices or Users.
2. On the Home tab of the ribbon select Import User Device Affinity.
3. Browse and select the CSV file containing the information that you want to import, and click Open. The format of the CSV file must be `<Domain\user name>,<Device NetBIOS name>`. Select the option This File Has Column Headings For Reference Purposes if you have the following as the first line of the CSV file: `users,devices`.
4. Check in the File Preview section of the Choose Mapping page of the wizard to see if the column mapping is configured correctly, as shown in Figure 10.37, and click Next twice. Click Close after reviewing the results.

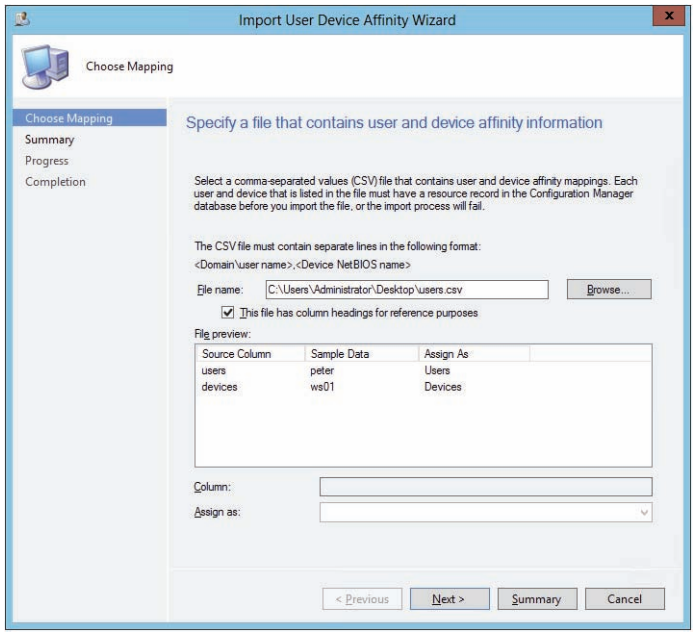


FIGURE 10.37 Check the column mapping.

Enable Users to Configure Their Primary Device

Another option is to configure the Configuration Manager 2012 site to let the users define their own user device affinities. This is done as follows:

1. From within the Configuration Manager console, select the Administration workspace, expand Overview, and select Client Settings.
2. Select the default client settings package or create a new client device user settings package. Then click Properties on the Home tab of the ribbon.
3. Select User And Device Affinity, and set the option Allow Users To Define Their Primary Devices to Yes. Setting the option to No will disable the feature.

From now on, the users can configure their user device affinity by selecting the I Regularly Use This Computer To Do My Work option in the My Devices tab of the Application Catalog website.

Pre-deploy User Applications

After configuring user device affinity for a client computer, the applications that are targeted to the primary user are pre-deployed automatically during deployment of the OS. Be sure to enable, while deploying the application to a user, the option Deploy Automatically According To Schedule With Or Without User Login, and set the Purpose to Required, as shown in Figure 10.38. You will find more information about deploying applications in Chapter 6, "Client Installation."

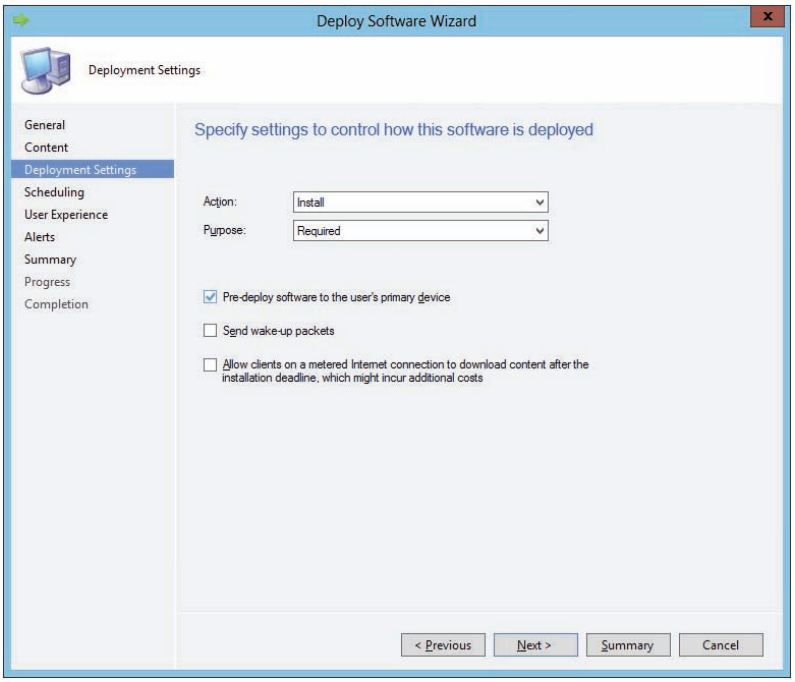


FIGURE 10.38
Configure deployment settings.

Deploying Windows To Go

Windows To Go is new for Window 8.*x* and gives you the ability to install your corporate domain-joined image from a USB-connected device. This can be a special USB stick or a special USB drive. To be able to install your corporate Windows 8.*x* image on the USB device, you need to follow these steps:

1. Create a task sequence for deploying Windows 8.*x*.
2. Create a prestaged media for the task sequence.
3. Create a Windows To Go creator package.
4. Update the task sequence to enable BitLocker.
5. Deploy the Windows To Go creator package and Windows 8.*x* task sequence.

Creating a Prestaged Media for the Task Sequence

Since you've already created a task sequence for deploying bare-metal computers, you can use it for the Windows To Go deployment.

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview, expand Operating Systems, and select Task Sequences.
2. Click Create Task Sequence Media from the Home tab of the ribbon and select Prestaged Media in the Create Task Sequence Media Wizard; then select Allow Unattended Operating System Deployment. Click Next.
3. Select Site-Based Media, click Next, and specify information for the media file, as shown in Figure 10.39.

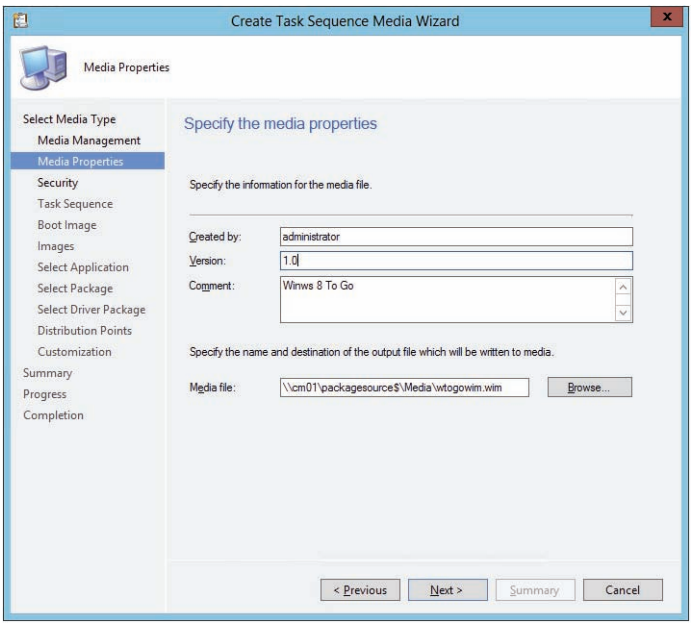


FIGURE 10.39 Create Task Sequence Media Wizard - Media Properties

4. Supply a media file to which the output is written and click Next.
5. Keep Enable Unknown Computer Support enabled and supply a strong password. Click Next.
6. Click Browse, select the Bare Metal Deployment task sequence created previously, and click Next.
7. On the Boot Image page, select a distribution point and management point that can be used by the boot media.
8. Select the distribution point on the Images page, and click Next.
9. Add an application that you want to install, as shown in Figure 10.40, and click Next.

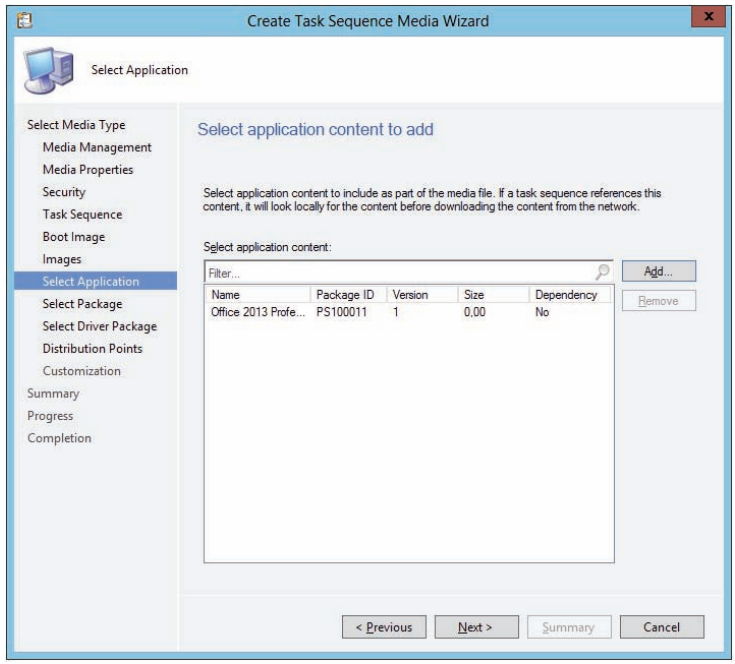


FIGURE 10.40
Create Task Sequence Media Wizard - Select Application

10. Add packages that you want to install and click Next.
11. Select driver packages that you need and click Next.
12. Select the distribution points you need and click Add. Click Next after adding the distribution points.
13. When enabling BitLocker on a Windows To Go device, you need a passphrase; this passphrase can be set with the variables in the Customization page of the wizard. Click the yellow starburst and add **`OSDBitLockerPIN`** as the name of the variable, as shown in Figure 10.41. Click OK and Next.

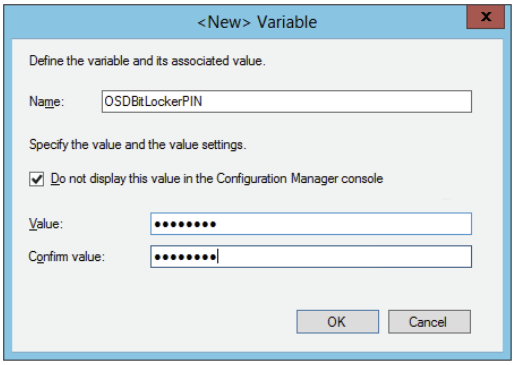


FIGURE 10.41
Add the *OSDBitLockerPIN* variable.

14. Review the Summary and click Next.
15. Click Close after the Create Task Sequence Media Wizard has completed successfully.

Creating a Windows To Go Creator Package

The next step in the process of creating a Windows To Go USB device is creating the Windows To Go creator package.

1. Copy the just-created WIM file to a folder in the package source share of your environment.
2. Copy the file `wtgcreator.exe`, which you can find in the `\OSD\Tools\WTG\Creator` folder in the program folder of your Configuration Manager 2012 installation, to the same folder in the package source share.
3. From within the Configuration Manager console, select the Software Library workspace, expand Overview, expand Application Management, and select Packages.
4. Click Create Package in the Home tab of the ribbon of the console. Supply a name, description, and manufacturer, and enable the This Package Contains Source Files option. Click Browse and browse to the just-created folder in the package source share with the WIM file and the `wtgcreator.exe` file. Click Next.
5. Select Standard Program and click Next. Supply a name and the command line that will provision the Windows To Go device. The command line must be in the format `WTGCreator.exe /wim:<wimfile>.wim`, as shown in Figure 10.42.
6. Select Program Can Run Only When A User Is Logged On, and configure the run mode as Run With Administrative Rights. Select the option Allow Users To View And Interact With The Program Installation. Click Next.
7. Configure the requirements for the platform that can be used to provision the device. Click Next.
8. Review the summary, click Next, and click Close after processing the changes.

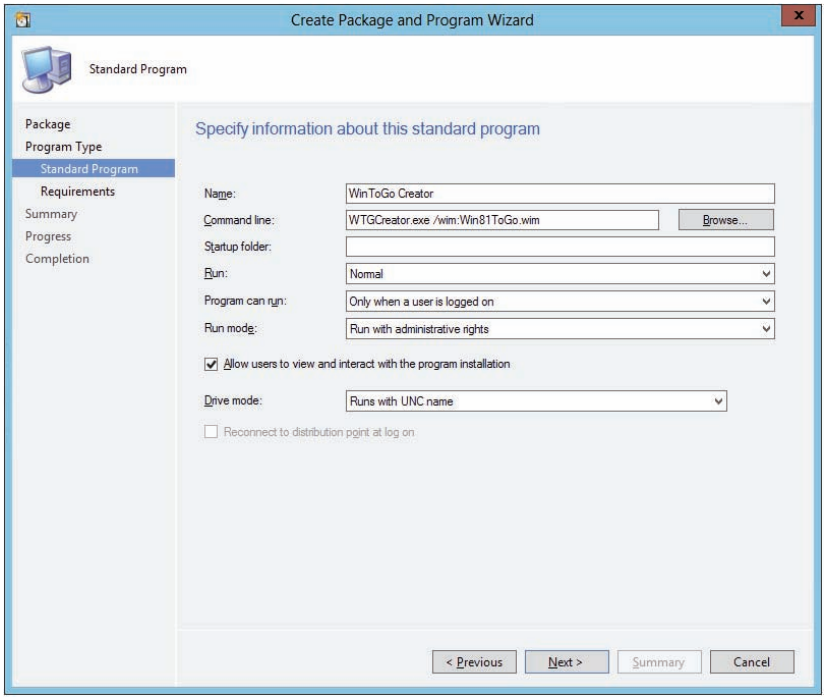


FIGURE 10.42
Create the Windows To Go Creator package.

After creating the package, be sure to distribute the package to the distribution points and deploy it to a collection with users who are allowed to provision the Windows To Go devices.

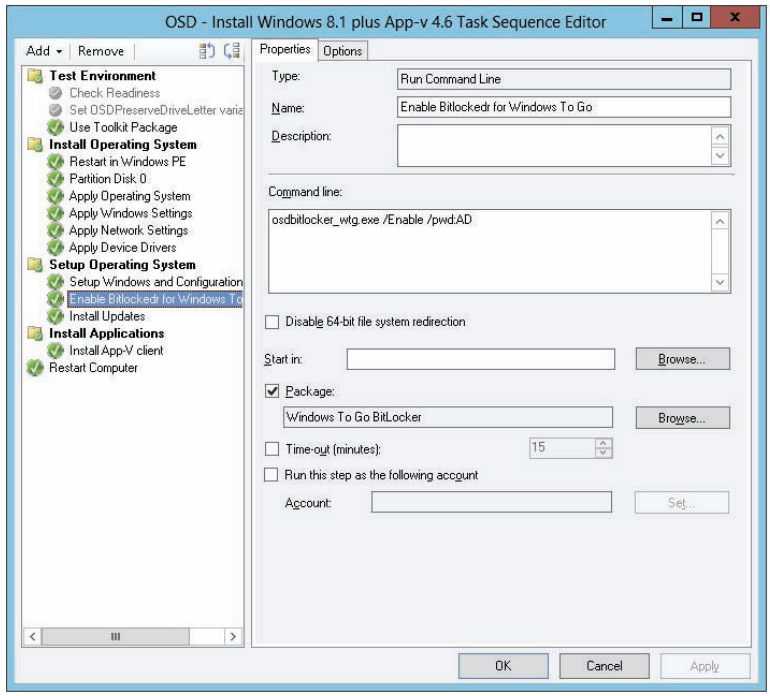
Update the Task Sequence to Enable BitLocker

The next step is to enable BitLocker for the Windows To Go devices. To do this, you need to create a package for the utility that allows you to enable BitLocker, and you need to change the task sequence:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview, expand Application Management, and select Packages.
2. Click Create Package in the Home tab of the ribbon of the console. Supply a name, description, and manufacturer, and enable the This Package Contains Source Files option. Use as the source folder `\OSD\Tools\WTG\BitLocker` in the program folder of your Configuration Manager 2012 installation.
3. Select Do Not Create A Program and click Next, Next, and Close.
4. From within the Configuration Manager console, select the Software Library workspace, expand Overview, expand Operating Systems, and select Task Sequences.

5. Select the task sequence that you will use to provision the Windows To Go device and click Edit in the Home tab of the ribbon.
6. Select the Setup Windows And ConfigMgr task and click Add ➢ General ➢ Run Command Line.
7. Supply a name and command line that will provision the Windows To Go device. The command line must be in the format `i386\osdbitlocker_wtg.exe/Enable/pwd:AD` when using the 32-bit operating system or `x64\osdbitlocker_wtg.exe/Enable/pwd:AD` when using a 64-bit operating system. The `/pwd` parameter can either be None for not saving the `BitLocker PIN or AD` for storing the `BitLocker PIN` in Active Directory.
8. Enable the Package option, click Browse, and select the earlier-created BitLocker package, as shown in Figure 10.43.

FIGURE 10.43
Edit the task sequence to enable BitLocker.



9. Click the Options tab of the BitLocker task in the task sequence and click Add Condition ➢ Task Sequence Variable. Supply **`_SMSTSWTG`** as a variable, **`equals`** as the condition, and **`True`** as the value. Click OK.
10. Click OK after adding the condition.

Deploy the created task sequence to a collection with devices that can be used to provision Windows To Go.

Running the Windows To Go Package

The next step is to start the deployed Windows To Go creator package from a Windows workstation. By doing this, the Prestaged Media WIM file will be installed on the device that you will be using for Windows To Go.

1. Plug in the USB device and unlock it if necessary.
2. Go to the Software Center in the Start screen and install the Windows To Go creator package. After the Windows To Go creator software is started, you need to select the LUN on the device that has enough space to hold the Windows To Go installation, as shown in Figure 10.44. Click Next.

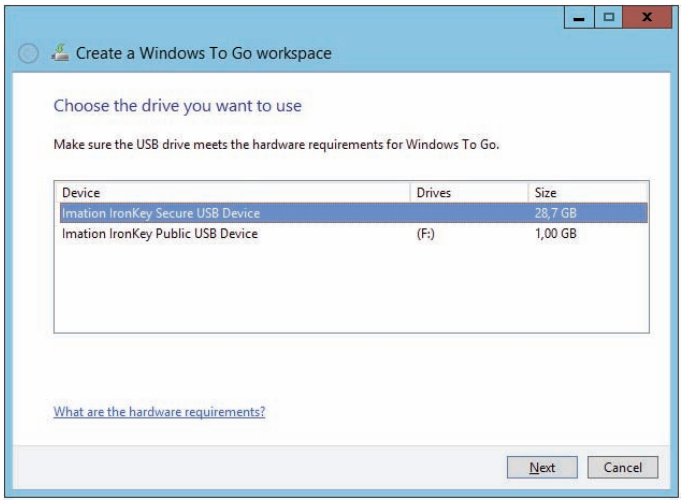


FIGURE 10.44 Select the LUN to deploy Windows To Go to.

3. Click Create to create the Windows To Go workspace, as shown in Figure 10.45. The created task sequence media will be used to provision, in this case, the Imation Ironkey W500.

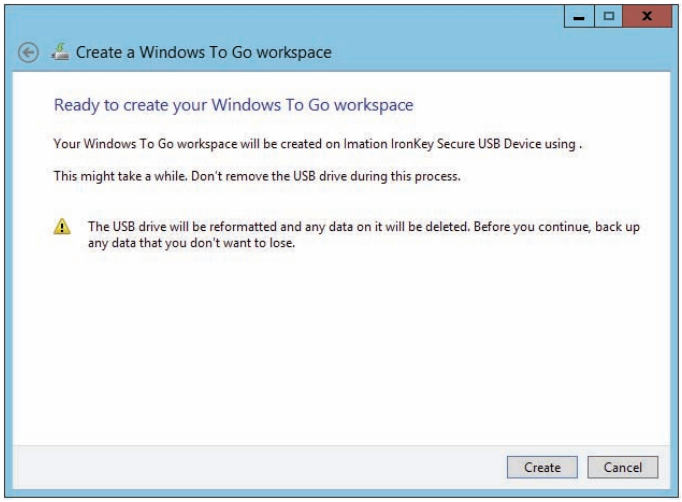


FIGURE 10.45 Click Create to create the Windows To Go workspace.

4. After the provisioning step is finished, click Finish.

   The next step is to finish the installation of the Windows To Go workspace. You will need to boot from the Windows To Go USB device into the prestaged media environment and start the deployed Windows 8.1 task sequence. This will start the actual installation and configuration of Windows To Go on the USB device. When this process is finished, you are good to go.

Be Sure to Change the Boot Sequence

When provisioning the Windows To Go environment, you need to make sure that the workstation on which you are doing this is configured to boot first from your USB device. The workstation must restart several times during the installation of the Windows To Go workspace.

Microsoft Deployment Toolkit 2013

The Microsoft Deployment Toolkit 2013 is a solution accelerator that can be integrated with Configuration Manager 2012 R2. The integration gives you the ability to smooth your deployment process with the scripts that come with the Deployment Toolkit. Let's configure the Microsoft Deployment Toolkit integration and see what it offers us when deploying operating systems.

The Microsoft Deployment Toolkit includes extra deployment scenarios that are built with a Task Sequence Wizard, such as the following:

Replace Hardware Scenario This scenario enables you to capture the user state from an old client computer and place it while deploying the new operating system on the new client computer.

Server Deployment Scenario This scenario allows you to deploy Windows-based servers and their roles.

User-Driven Installation Scenario This scenario allows your users to use a simple User Driven Installation (UDI) Wizard to initiate and customize an OS deployment on their PCs that's tailored to their individual needs.

The wizard uses existing supporting packages like the boot image, the Microsoft Deployment Toolkit, or the User State Migration Package or allows you to create new packages while configuring the task sequence.

Installing Microsoft Deployment Toolkit 2013

The Microsoft Deployment Toolkit is a free tool that you can download from the Microsoft Download site. Install the `MicrosoftDeploymentToolkit2013_x64.msi` or `MicrosoftDeploymentToolkit2013_x86.msi` file on your site system. It's a straightforward

Next, Accept License Agreement, Next, Next, Next, Install, Finish installation. You need to install the Microsoft Deployment Toolkit on every site server that you want to integrate with.

Integrating the Deployment Toolkit

To be able to use the deployment intelligence of the Microsoft Deployment Toolkit in Configuration Manager 2012 R2, you need to integrate the Deployment Toolkit with Configuration Manager. This is done by following these steps:

1. After installing the Microsoft Deployment Toolkit 2013 on your site system, go to the Start screen.
2. Click Configure ConfigMgr Integration to start the integration tool.
3. Configure the integration as shown in Figure 10.46.
4. Select Install The MDT Console Extensions For System Center 2012 R2 Configuration Manager and Add The MDT Task Sequence Actions To A System Center 2012 R2 Configuration Manager Server. Next, configure the Site Server Name and Site Code fields, and click Next.
5. Review the summary, and click Finish.

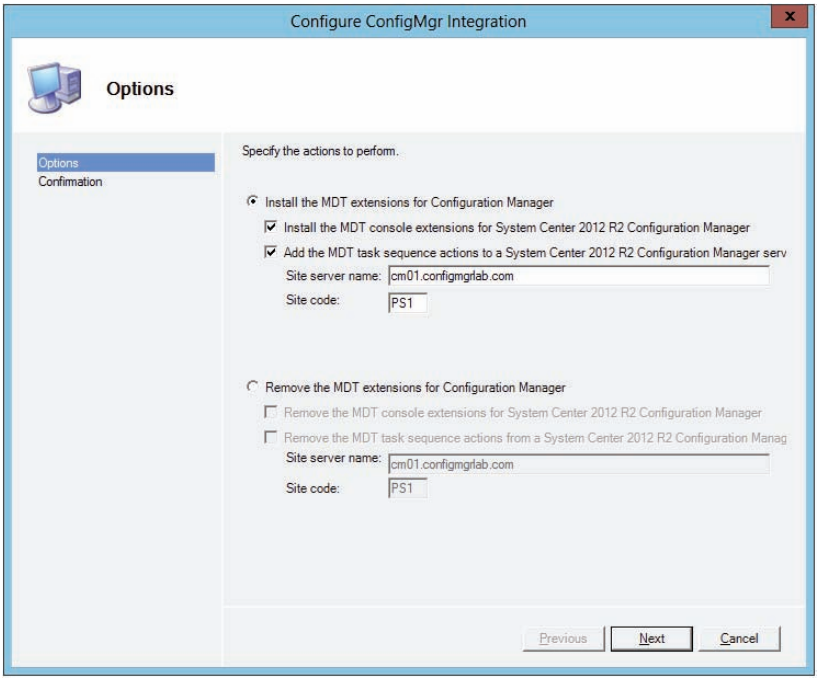


FIGURE 10.46
Configure the integration

Creating a New Boot Image

This is an optional step since more and more extras of the Microsoft Deployment Toolkit are moving to native Configuration Manager features. Follow the next steps to re-create the Microsoft Deployment Toolkit boot images. You can also create a boot image with the Microsoft Deployment Toolkit integration features while creating a new Microsoft Deployment Toolkit task sequence. Create a boot image for both x86 and x64 platforms.

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Boot Images.
2. Click Create Boot Image Using MDT on the Home tab of the ribbon, and supply the UNC path to the location where you want to store the boot image; click Next.
3. Supply a name, version, and comments, and click Next.
4. Select the platform for which you are creating the boot image, select the Scratch Space value from the dropdown list, as shown in Figure 10.47, and click Next. Scratch Space is a RAM drive that is used during OSD.

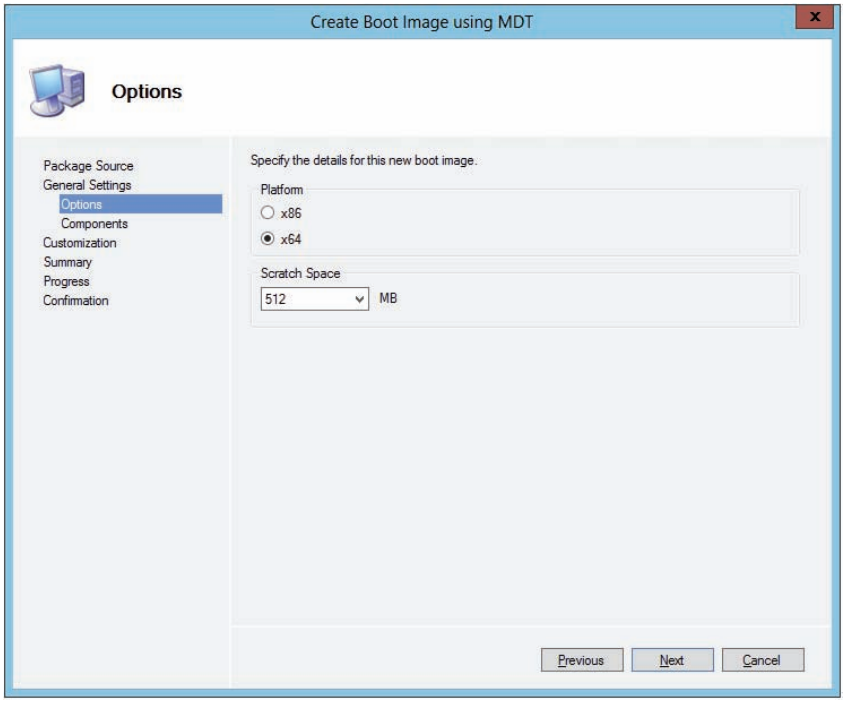


FIGURE 10.47 Configure the platform and scratch space.

5. Configure the optional languages and components like MDAC/AO support and PPPoE support and click Next.
6. Configure the customizations, such as the pre-execution hook, custom background image, and command support.

7. Click Next to review the summary.
8. Click Next after reviewing the summary, and click Finish after creating the custom boot image; this process can take a while.
9. Be sure to enable the boot image for PXE support and the deployment of the boot image to the distribution points.

Creating a Deployment Toolkit Task Sequence

After creating the optional Microsoft Deployment Toolkit boot images, you need to create a task sequence that you can use to deploy the operating system. In this example we will use the client replace scenario, which consists of two task sequences: the Client Replace task sequence and one based on the new computer scenario. The new computer scenario is like the bare-metal scenario, but we also use the User State Migration Toolkit to bring back the user state.

1. From within the Configuration Manager console, choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Click Create MDT Task Sequence on the Home tab of the ribbon, and select the Client Replace Task Sequence option. Then click Next.
3. Give the task sequence a name, supply comments, and click Next.
4. Select an existing boot image, or create a new boot image using the Create A New Boot Image Package option. Click Next.

   The first time you create a Microsoft Deployment Toolkit task sequence, you will need to create a Microsoft Deployment Toolkit Files package.
5. Select this option and supply a package source folder, as shown in Figure 10.48.

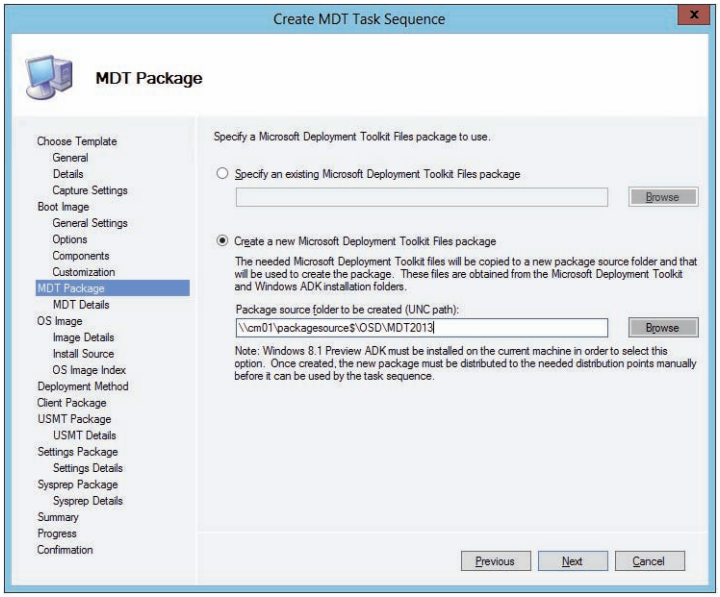


Figure 10.48 Create a new Microsoft Deployment Toolkit Files package.

The next time you create a Microsoft Deployment Toolkit task sequence, you can select the Microsoft Deployment Toolkit 2012 package.

6. Click Next.
7. Now you need to supply information about the package. Fill in the name, version language, and manufacturer, and click Next to proceed.
8. Select the User State Migration Tool package, and click Next.
9. Select Create A New Settings Package For This Operating System Deployment, supply the UNC path, and click Next.
10. Supply information about the package. Fill in the name, version language, and manufacturer, and click Next to proceed.
11. Review the summary and click Next. Click Finish after you've finished creating the packages and the task sequence.

After creating the Client Replace task sequence, you will need to create a task sequence based on the new computer scenario.

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Click Create MDT Task Sequence on the Home tab of the ribbon, and select the Client Task Sequence option. Then click Next.
3. Give the task sequence a name, supply comments, and click Next.
4. Supply the domain information, the account that has permissions to join the domain, and the Windows settings, and then click Next.
5. Select This Task Sequence Will Never Be Used To Capture An Image, and click Next.
6. Select an existing boot image, or create a new boot image using the Create A New Boot Image Package option. Click Next.
7. Select the Microsoft Deployment Toolkit 2012 package that you created earlier, and click Next.
8. Select the operating system image you want to deploy, as shown in Figure 10.49, and click Next.
9. Select Perform A "Zero Touch Installation" OS Deployment, With No User Interaction, and click Next.
10. Select the Configuration Manager Client 2012 package, and click Next.
11. Select the User State Migration Tool package, and click Next.
12. Select Create A New Settings Package For This Operating System Deployment, supply the UNC path, and click Next.
13. Supply information about the package. Fill in the name, version language, and manufacturer, and click Next to proceed.

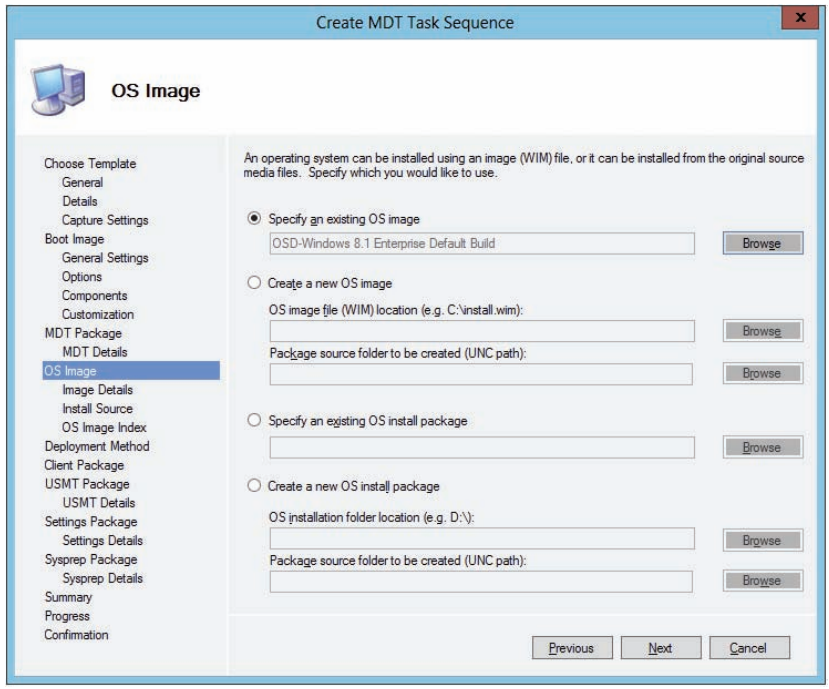


Figure 10.49
Select or create the operating system image you want to deploy.

14. Select No Sysprep Package Is Required, and click Next.
15. Review the summary, and click Next.
16. After the task sequence has been created, click Finish.

Using a Replace Scenario

The next step in creating a replace scenario for a computer is creating a computer association. This way the User State Migration Tool knows where to place the user state after installing the new computer.

1. From within the Configuration Manager console, select the Assets And Compliance workspace, and expand Overview ➢ Devices.
2. Click Import Computer Information on the Home tab of the ribbon.

   This will allow you to enter a single computer or import many systems from a comma-separated values (CSV) file.
3. Select the option Import Single Computer and click Next. This will bring up the Single Computer page.

You must enter the computer name along with either the MAC address or the SMBIOS GUID. The computer name is just how the machine will appear in the collections, not what the actual computer will be named.

4. Fill in the appropriate information, and select the source computer.

   This creates an association with the old computer, and the User State Migration Tool knows where to get the user state.

5. After configuring, click Next.
6. On the Data Preview page, check the information and click Next.
7. Next, you'll see the Choose Target Collection page. Here specify which collection you want to add to this new machine.

   It is extremely valuable to put all the new computer installs into the same collection, which is used exclusively for new computer deployment.

8. Click Next.
9. After specifying the collection, you will see the Summary page. Review the information, click Next, and then click Close on the Finish page.

Next, you need to deploy the task sequences you just have created. The Client Replace task sequence must be deployed to a collection that is especially created for the old client computers. Then you need to deploy the New Computer task sequence to the collection that was specially created for the new computers. The deployment must support booting from PXE, as you learned in the "Deploying the Task Sequence" section earlier in this chapter.

Deploying a Virtual Hard Drive

With Configuration Manager 2012 you can deploy your images to a VHD that can be maintained by Configuration Manager and uploaded to a System Center 2012 R2 Virtual Machine Manager library. This is another example of the fact that Configuration Manager can be used to service the datacenter.

Deploying a virtual hard drive is done in two steps:

1. Create a VHD task sequence.
2. Create a virtual hard drive.

Creating a VHD Task Sequence

To be able to install an existing reference operation system image to a virtual hard drive, you need to create a special task sequence:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Task Sequences.
2. Click Create Task Sequence on the Home tab of the ribbon, and select the option Install An Existing Image Package To A Virtual Hard Drive in the Create Task Sequence Wizard. Click Next.

3. Supply a name and description for the task sequence, and select a boot image that will support the operating system that you want to deploy. Click Next.
4. On the Install The Windows Operating System page, select the image package by browsing to the correct image. Supply a product key and be sure to enter a local administrator password.
5. On the Configure Network page, select the domain or workgroup to join.

   If you select to join a domain, you can specify which OU to put the computer in once it joins the domain. You also will need to specify the account that has permission to join computers to a domain. The Configuration Manager Network Access account is often used to join the computer to the domain. You need to delegate this access to the user account. Verify the account by testing the connection after configuring the account.
6. Click Next to continue. On the Install Configuration Manager Client page, specify any additional installation properties. Click Browse if you do not want to use the default Configuration Manager 2012 client package.
7. Click Next to add applications to the task sequence. Click Next to review the summary.
8. After reviewing the summary, click Next and then Close to complete the creation of the task sequence. As always, be sure that all the related content is distributed to your distribution point (groups).

Creating a Virtual Hard Disk

The next step is creating the actual virtual hard disk. To do this, you need to run the Create Virtual Hard Disk Wizard from the Configuration Manager 2012 R2 console on a machine with the Hyper-V Role and Management console installed.

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Virtual Hard Disks.
2. Click Create Virtual Hard Disk on the Home tab of the ribbon. If this option is grayed out, you do not have the Hyper-V role or administrative tools installed.
3. Supply a name, version, comments, and a path to the VHD file, as shown in Figure 10.50; then click Next.
4. Select the task sequence created in the previous section and click Next.
5. Select the distribution point where all packages are available and click Add. Click Next to continue.
6. Add customizations for the task sequence if necessary and click Next.
7. Review the summary and click Next to start the VDH creation process, as shown in Figure 10.51.

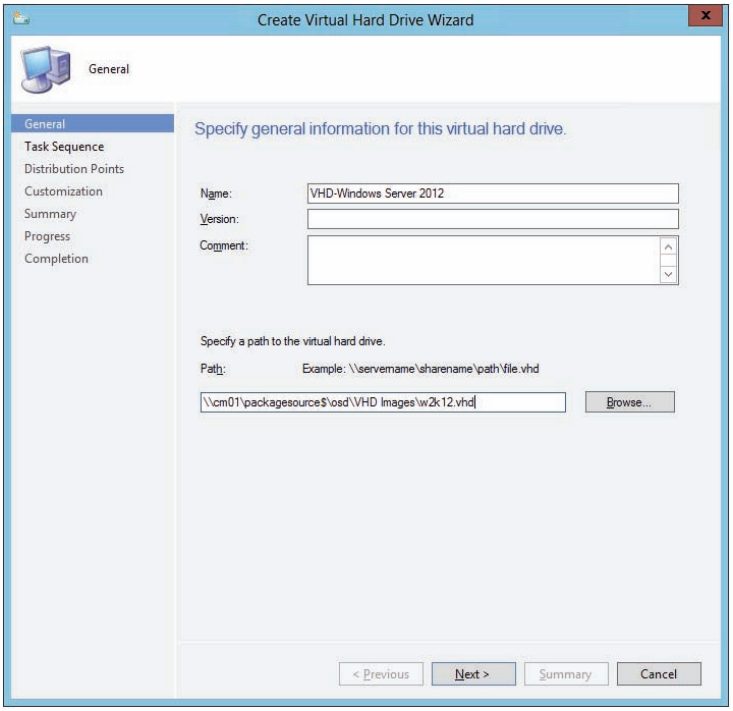


FIGURE 10.50 Specifying general information for the VHD

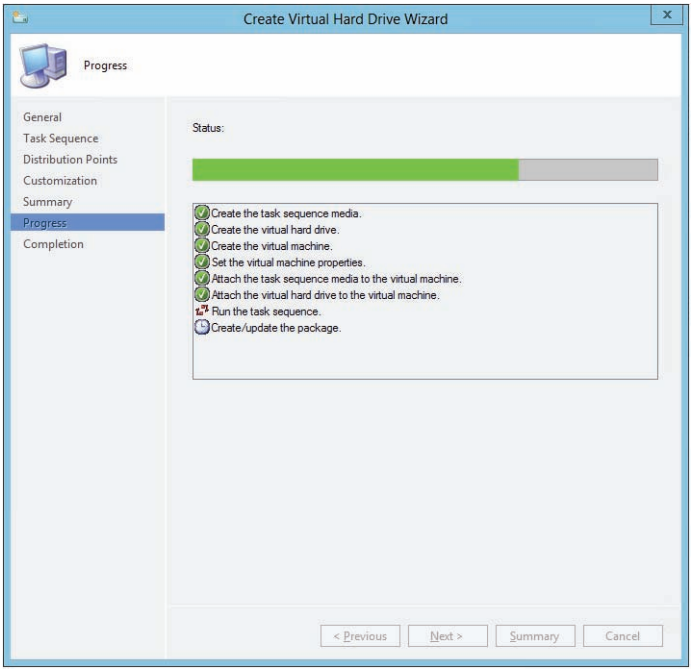


FIGURE 10.51 VHD creation process

In the backend, a virtual machine with the virtual hard disk is created in Hyper-V and the task sequence is started in this virtual machine. The virtual machine that it creates has a random name, as shown in Figure 10.52.

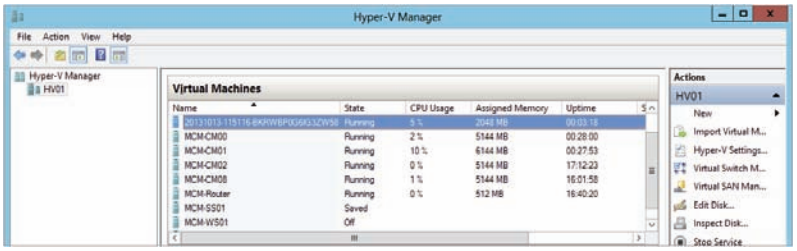


FIGURE 10.52
The created virtual machine in Hyper-V

After the task sequence is finished, the virtual machine will be deleted and the VHD file will be stored in the share that you have defined.

8. Click Close once the VHD is created.

Managing the Virtual Hard Disk

Now that you have a deployed virtual hard disk in your Configuration Manager 2012 R2 environment, you want to do something with it. There are several options; you can use it as an existing virtual hard disk in Hyper-V when creating a virtual machine manually or upload it in the System Center 2012 R2 Virtual Machine Manager library. Uploading the VHD is done as follows:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Virtual Hard Disks.
2. Select the created virtual hard disk and click Upload To Virtual Machine Manager in the Home tab of the ribbon. You need to install the Virtual Machine Manager console to be able to upload the VHD.
3. Supply the VMM server name, select the VMM library share, and click Next. Review the summary, click Next, and click Close after completing the upload.

You can also modify the VHD from the Configuration Manager 2012 R2 console. For instance, here you can change the task sequence:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Virtual Hard Disks.
2. Select the created virtual hard disk and click Modify Virtual Hard Disk. This kicks off the same wizard for creating the VHD, but you cannot change the path and name of the VHD, as shown in Figure 10.53.

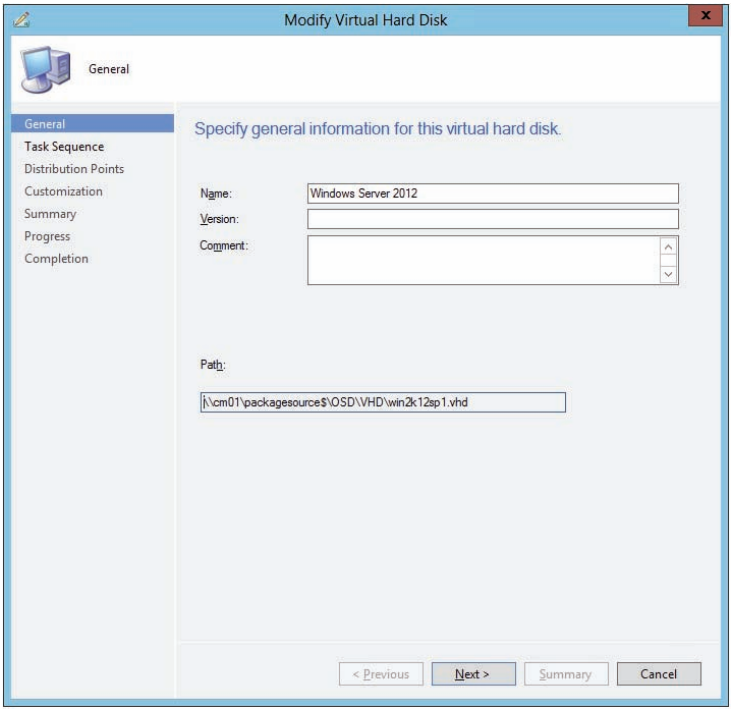


FIGURE 10.53 Modifying the virtual hard disk

Servicing Your Operating System Images and VHDs Offline

In Configuration Manager 2007 you needed a tool called Deployment Image Servicing and Management (DISM)—a command-line tool used to maintain and update your images offline. Configuration Manager 2012 R2 comes with the ability to update your operating system images from the console. This feature uses the software update point and software update deployments that you configured earlier. Follow these steps if you want to update a WIM image:

1. From within the Configuration Manager console, select the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Images.
2. Select the operating system you want to update, and click Schedule Updates on the Home tab of the ribbon.
3. Select the updates that you want to install in the Windows image, as shown in Figure 10.54, and click Next.
4. Select the schedule (as soon as possible or a custom schedule) for the update process, and click Next.
5. Review the summary, and click Next. Click Close when the process of scheduling the updates is finished.

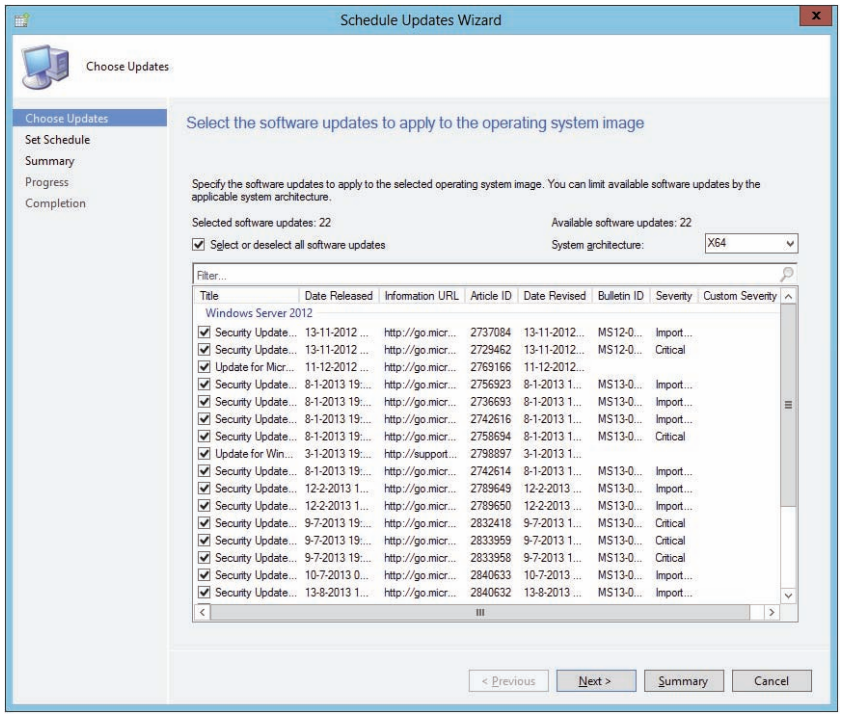


FIGURE 10.54
Select the updates that you want to install.

The process of updating the Windows image can take a while; you can view the status of the process in the Scheduled Update Status column in the Configuration Manager console. Once the update is finished, you can see the installed updates in the console, as shown in Figure 10.55.

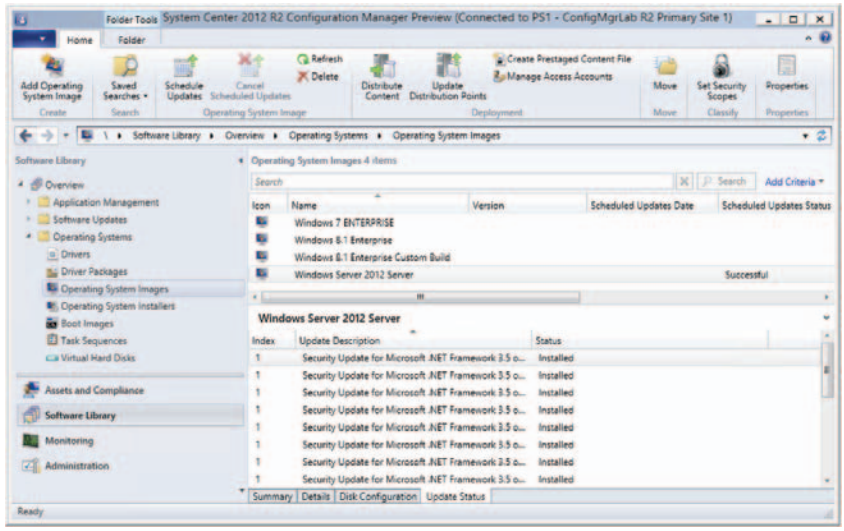


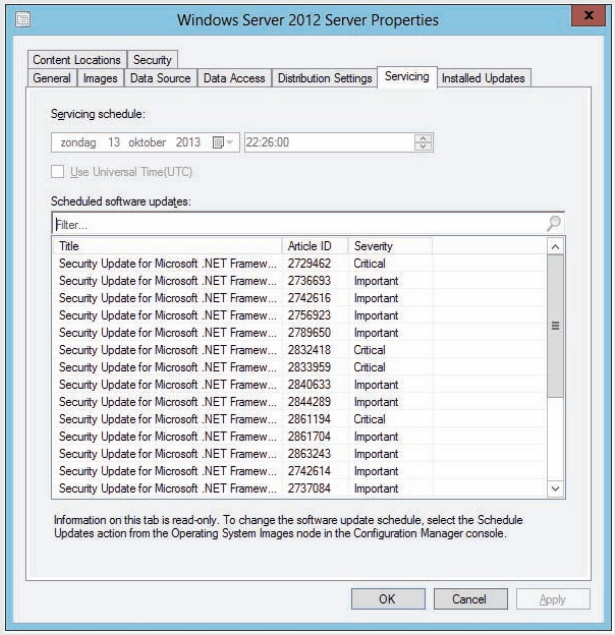
FIGURE 10.55
View the installed updates in the Windows image.

Besides installing software updates offline to operating system images, you can also schedule the installation of updates to virtual hard disks. The Schedule Updates wizard will walk you through the process.

Monitoring and Troubleshooting Offline Servicing

You can use the `OfflineServicingMgr.log` file in the logs folder of the Configuration Manager 2012 installation folder to monitor or troubleshoot while servicing your images offline.

You are also able to monitor the offline servicing by accessing the properties of the WIM image and viewing the Servicing tab, as shown in the following image. In addition, you can change the schedule if you have scheduled offline servicing.



Support for Legacy Boot Images

Existing or manually created boot images based on Windows PE 3.1 can be added to Configuration Manager 2012 R2 to support the unattended installation of legacy operating systems like Windows XP or Windows 7. Configuration Manager 2012 R2 is able to distribute the boot images only to the distribution points; you cannot use Configuration Manager 2012 R2 to add drivers or make other changes to the Windows PE 3.1 boot images.

Walk through the following steps to create a custom Windows PE 3.1 boot image:

1. Download and install the Windows Automated Installation Kit (WAIK) 3.1 on a remote system.
2. Start the Deployment and Imaging Tools Environment from the Start menu or Start screen.
3. Create a folder named **`c:\winpe_x86`** and start the command **`copype.cmd x86 c:\winpe-x86`**.
4. Copy and rename (to `boot.wim`) the default copied WinPE boot image to `c:\winpe-x86\iso\sources` with the following command: **`copy c:\winpe-x86\winpe.wim c:\winpe-x86\iso\sources\boot.wim`**.
5. Mount the `boot.wim` image so that you are able to make changes, and then dismount it with the following command: **`Dism /mount-wim /wimfile:C:\winpe-x86\ISO\sources\boot.wim /index:1 /MountDir:C:\winpe-x86\mount`**.
6. Now that the boot image is mounted and accessible through `c:\winpe-x86\mount`, you can modify it. You want to add WMI (WinPE-WMI), Scripting (WinPE-Scripting), and Windows Deployment Services (WinPE-WDS-Tools) support. Adding support is done as follows:
   - `Dism /image:C:\winpe-x86\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-wmi.cab"`
   - `Dism /image:C:\winpe-x86\mount /Add-Package /PackagePath: "C:\Program Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\en-us\winpe-wmi_en-us.cab"`
   - `dism /image:C:\winpe_x86\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK \Tools\PETools\x86\WinPE_FPs\winpe-scripting.cab"`
   - `dism /image:C:\winpe-x86\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK \Tools\PETools\x86\WinPE_FPs\en-us\winpe-scripting_en-us.cab"`
   - `dism /image:C:\winpe-x86\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK \Tools\PETools\x86\WinPE_FPs\winpe-WDS-Tools.cab"`
   - `dism /image:C:\winpe-x86\mount /Add-Package /PackagePath:"C:\Program Files\Windows AIK \Tools\PETools\x86\WinPE_FPs\en-us\winpe- WDS-Tools_en-us.cab"`
7. After making changes to the boot image, you need to commit those changes to the `boot.wim` file, this is done with the following command: **`Dism /unmount-Wim /MountDir:C:\winpe-x86\mount /Commit`**.
8. After committing the changes, you need to copy the boot image to your package source and import the boot image to Configuration Manager. You need to do the same for the x64 boot image. Use the imported images only for the task sequences that need the custom legacy boot images.

For a complete guide to creating custom boot images, see the TechNet article "Walkthrough: Create a Custom Windows PE Image": `http://technet.microsoft.com/en-us/library/dd744533(WS.10).aspx`.

Maintaining the User State

When you browse to the User State Migration node in the Assets And Compliance workspace, as shown in Figure 10.56, you can manage computer associations. In this workspace you can create new computer associations, as mentioned earlier, see recovery information, find information about the user state migration, or specify the user accounts.

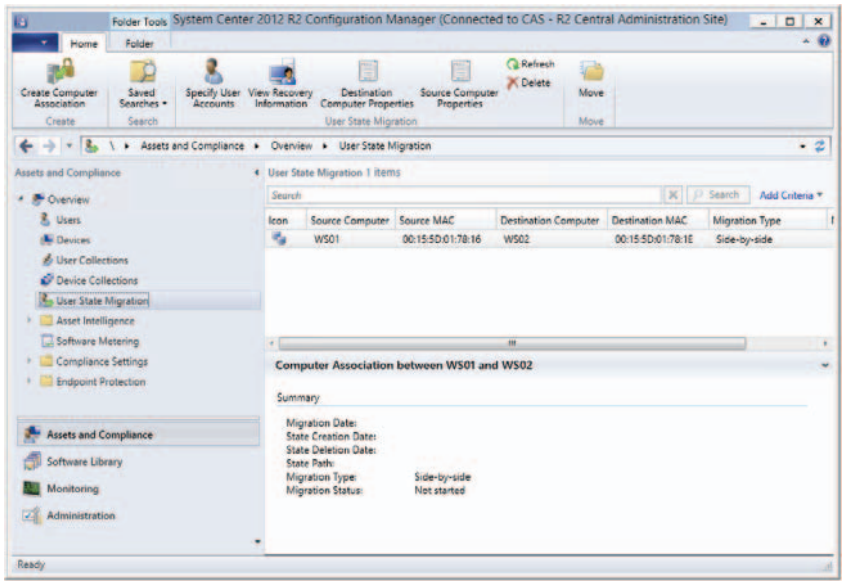


FIGURE 10.56 Managing the user state

Specifying the user accounts is done as follows:

1. From within the Configuration Manager console, choose the Assets And Compliance workspace and expand Overview ➢ User State Migration.
2. Select the User State Migration item, and click Specify User Accounts to add user accounts for which data needs to be migrated.
3. Click the starburst icon, and on the Add User Account screen click Browse. Search for the user and click OK twice.
4. Click OK to set the user account to migrate.

From this view you can also create computer associations when, for instance, migrating user state data from one computer to an existing computer that is being reinstalled.



Real World Scenario

Assigning Many Computers to the Bare-Metal Deployment

George T. Management sends an email to the help desk stating that his department just ordered 10 new machines with no operating system and that he wants them all configured by the end of the day with the same image that was used on his machine. The list of 10 machines was included in the email.

You meet with your Configuration Manager team and decide that the best way to do this is to use Configuration Manager to push the image out using the PXE service point that has already been used in the environment.

So, you open the Configuration Manager console, choose the Assets And Compliance workspace, expand Overview ➢ Devices, and click Import Computer Information on the Home tab of the ribbon. On the Import Computer Information page, you select Import Computers Using A File, and click Next. On the Choose Mappings page, you click Browse to browse the comma-separated file that Mr. Management sent you containing the list of computers on which you need to deploy the new operating system.

After you import the file and assign the data mappings, you click Next. Then you verify that the data is correct on the Data Preview page and add these systems into the bare-metal collection created earlier with the Windows 7 build already assigned. Finally, you click Finish to add the members to the collection. Configuration Manager will then deploy the new operating system when the machines are powered on and booted up in PXE boot.

The Bottom Line

Specify a Network Access account. The Network Access account is the account Configuration Manager will use to access the system while running WinPE.

Master It How do you specify the Network Access account?

Enable PXE support. PXE support in Configuration Manager is used to begin the operating system deployment process. The PXE feature responds to Configuration Manager clients making PXE boot requests.

Master It How do you set up PXE support?

Update the driver catalog package. The driver catalog allows you to add drivers to the already created packages and images you have within your organization so you are not constantly re-creating your images when you get a new machine in your environment.

Master It How do you update the driver catalog package?

Update an image from the console. In the past it was a big issue to keep your images up to date; no easy procedure existed. In Configuration Manager 2012 a feature called Schedule Updates exists to update your Windows images.

Master It How do you update your Windows images?



Chapter 11

Inventory and Software Metering

The ability to provide detailed hardware and software inventory is one of the core features of Configuration Manager. Many companies rely on this data to obtain a clear understanding of the configuration of the computers in the environment. Hardware inventory gathers information from your systems such as the processor type, computer manufacturer, and amount of installed memory. Software inventory can gather lists of file types and versions that are installed on your computers. Combining this data with the extensive information in the Asset Intelligence knowledge base covered in Chapter 12, "Asset Intelligence," provides value, so Configuration Manager becomes a valuable source of information about the computer infrastructure.

Software metering, the second major topic in this chapter, allows you to collect information on software usage to assist in managing software purchases and licensing. With this feature, you can report on the software that is being used in your environment and determine which users are running particular programs. You can also find software that is installed but isn't being used, and you can report on software license requirements and other items related to license management.

In this chapter, you will learn to

- Configure and manage Software Inventory
- Configure and manage Hardware Inventory
- Configure and manage Software Metering

Inventory in Configuration Manager 2012

Gathering inventory data is considered one of the most important features of any enterprise management system. The inventory data that is gathered is often used to create reports, queries, and collections. One thing that is important to know is that the inventory data is not "live" data, because it is based on the latest inventory scan and could potentially be several days or weeks old. When a Configuration Manager client performs an inventory scan and submits the data to the client's management point, the management point will verify the data, send it to a Configuration Manager site server, and then write it to the Configuration Manager database. Once the data is in the database, it can be used in many ways.

- You can create queries that target computers based on their hardware configuration or installed software. You can use these queries to be proactive in preventing problems such as low hard disk space. Using inventory data for this proactive step may not be as important as it may have been in previous versions because you can perform checks in real-time during application deployments with the usage of global conditions.
- You can create queries that identify computers that do not have your organization's standard antivirus program installed. You can then use these search criteria to create a collection and then target that collection with an application deployment that will install the enterprise antivirus product.
- You can create reports showing hardware configuration and software installations that management can use to evaluate and improve the current computer environment.

Once the Configuration Manager client is installed, the first inventory is always a full inventory scan. Once it has been completed, all subsequent scans will send only *delta* inventory information, identifying what has changed. Delta inventory records are processed in the order in which they are received at the Configuration Manager site server. If for some reason a delta inventory is received from a client that is not in the database (such as a reimaged or new client, for example), the site server will delete the delta inventory and ask for a full inventory from that client the next time a scheduled scan is run.

Configuration Manager provides only limited support for computers that can boot up two or more operating systems. Configuration Manager clients can be discovered in multiple boot states, and the clients can be installed on each boot state. Inventory that is collected from these computers, however, will be from only the operating system that was running when the inventory scan was run.

Hardware inventory scanning will give you such information as disk space, video card type, memory installed, and much more. Configuration Manager 2012 uses Windows Management Instrumentation (WMI) to gather the needed data, and once you have learned the basics of WMI, you will find it fairly easy to modify the default hardware inventory settings.

Software inventory scanning will give you such information as the software installed, file types, and the versions of software. Unlike previous versions of Configuration Manager, in Configuration Manager 2012 the client is not configured to scan for any file types by default. The software inventory process can also collect files and store them on the primary site server, but this feature is rarely used because the collected files could create significant network usage and also consume a large amount of disk space on site servers.

Collecting Hardware Inventory

Hardware Inventory collects data from clients by querying several data stores of information that are on computers, such as the registry and WMI. The Hardware Inventory Client Agent doesn't query all WMI classes; it only pulls the information that is defined in the client settings assigned to the client. As you learned in Chapter 6, "Client Installation," you can have multiple client settings and assign them to different collections. Inventory scans are done on the schedule you configure in the client settings. Unless there is a problem with the client, only delta inventories will be collected after the first inventory. This greatly decreases the network traffic required by client inventory reporting because deltas are usually only a small percentage

of the size of a full inventory from a client. With every hardware inventory collection done on a client, Configuration Manager updates the site database with the current inventory while keeping a history of the previous information. You can view the current and historical inventory information in queries, reports, and Resource Explorer.

Hardware Inventory will also collect certain basic information about a client's installed software. This information is gathered from the registry. By using the software inventory, however, you can get a larger amount of and much more detailed information about the software that is present on client computers.

What Defines Hardware Inventory?

Configuration Manager gathers information about clients based on the settings defined in the client settings and the content of the `configuration.mof` (managed object format) file stored on the primary site server in the *<Folder where Configuration Manager is installed>*`\inboxes\clifiles.src\hinv` folder.

The configuration.mof File

The `configuration.mof` file defines the data classes to be inventoried by the Hardware Inventory Client Agent. Data classes can be created to inventory existing or custom WMI repository data classes or registry keys found on clients.

This file also defines and registers the WMI providers used to access computer information during hardware inventory. Registering providers defines the type of provider to be used and the classes that the provider will support. WMI can access only registered providers, so that applies to the Hardware Inventory Client Agent as well. The `configuration.mof` file can't be used to register new providers for clients. New or custom providers must be sent to clients to be compiled manually before they can be added to hardware inventory.

When Configuration Manager clients request computer policies as part of their policy polling interval, the `configuration.mof` file is part of the policy that clients download and compile. When you add, modify, or delete data classes from the `configuration.mof` file, clients will automatically compile those changes the next time the client compiles a computer policy that it receives.

Later in the chapter you'll get hands-on practice in modifying `configuration.mof` to extend the information collected in hardware inventory.

The Client Settings

Unlike in previous versions of Configuration Manager, you now have a graphic interface in the Configuration Manager console, as shown in Figure 11.1, to edit the reporting classes used by the inventory process. In Configuration Manager 2007 and previous SMS versions, you would modify the `sms_def.mof` file to define whether specific client data class information is reported. In Configuration Manager 2012, you either use the default client settings or create custom client settings to enable and disable reporting classes. The reporting classes are based on the WMI data classes that are on clients by default or have been added after the `configuration.mof` file has been modified.

This reporting class information in the client settings is converted to a reporting policy that is downloaded to clients as part of their computer policy polling download. After the client has finished compiling the new reporting policy, the reporting information is stored in

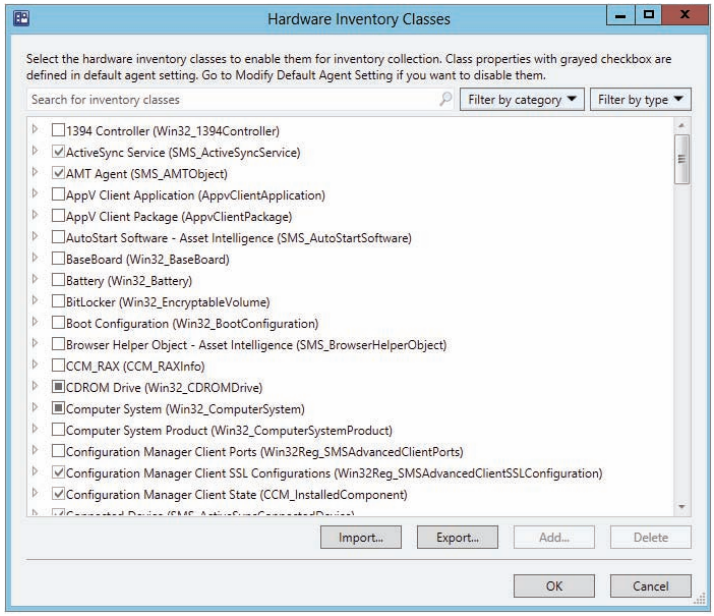


FIGURE 11.1 Default Hardware Inventory settings

the client WMI repository in the `InventoryDataItem` class of the `Root\CCM\Policy\Machine` WMI namespace. Unlike the `configuration.mof` file, the inventory client settings file is never sent to clients directly. Only the policy generated by the client settings is actually compiled by Configuration Manager clients.

Later in the chapter you will see several examples on how to extend hardware inventory.

The Default Hardware Inventory Reporting Classes

The default client settings have some reporting classes enabled. These default classes might change depending on what version of Configuration Manager and which service pack you have installed and on whether you have enabled classes for Asset Intelligence. Here is an example of the hardware inventory data classes that are enabled by default in Configuration Manager 2012 R2 with Asset Intelligence classes enabled:

- ActiveSync Service
- AMT Agent
- AutoStart Software
- Browser Helper Object
- CDROM Drive
- Computer System
- Configuration Manager Client SSL Configurations
- Configuration Manager Client State
- Connected Device
- Desktop Monitor
- Disk Drives
- Disk Partitions

IDE Controller

Installed Applications (64)

Installed Applications

Installed Software — Asset Intelligence

Logical Disk

Memory

Mobile Device Client Agent Version

Mobile Device Computer System

Mobile Device Display

Mobile Device Installed Applications

Mobile Device Memory

Mobile Device OS Information

Mobile Device Password

Mobile Device Power

Modem

Motherboard

NAP Client

NAP System Health Agent

Network Adapter

Network Adapter Configuration

Network Client

Operating System

Parallel Port

PC BIOS

Physical Memory

PNP Device Driver

Power Capabilities

Power Configuration

Power Insomnia Reasons

Power Management Daily Data

Power Management Exclusion Settings

Power Management Monthly Data

Power Settings

Processor

Recently Used Applications

SCSI Controller

Server Feature

Services

Software Licensing Product — Asset Intelligence

Software Licensing Service — Asset Intelligence

System Console Usage — Asset Intelligence

System Console User — Asset Intelligence

Software Tag

Sound Devices

System Devices

System Enclosure

Tape Drive

TS Issued License

TS License Key Pack

USB Controller

USB Device

Video Controller

Virtual Application Packages

Virtual Applications

Virtual Machine (64)

Virtual Machine

Virtual Machine Details

Windows 8 Application

Windows 8 Application User Info

Windows Update Agent Version

Each one of these reporting classes has certain criteria enabled, and these represent the actual data classes that are being collected. Some reporting classes might have all their data classes being captured or only some of them. The best way to determine what is being inventoried during the hardware inventory process is to browse through the individual classes in the Configuration Manager console.

The Role of MIF Files in Hardware Inventory

Management information format (MIF) files can be used to extend hardware inventory information that is collected from clients. The type of information that can be collected by MIF files can be just about anything, depending on how the MIF file is structured. During a hardware inventory cycle, the information in a MIF file is added to the client inventory report and stored in the Configuration Manager site database, where it can be used just like default client inventory data. The two types of MIF files that can be used to extend hardware inventory in this way are NOIDMIF and IDMIF.

By default, NOIDMIF and IDMIF file information is not inventoried by Configuration Manager. For this information to be added to hardware inventory, you must enable one or both file types in the Hardware Inventory settings. When you do, Configuration Manager creates new tables or modifies existing tables in the site database to add the properties in NOIDMIF and IDMIF files. NOIDMIF and IDMIF files are not validated, so they can be used to alter tables that you don't want altered. Doing this runs the risk that valid data could be overwritten by invalid data or large amounts of data could be imported into the Configuration Manager database, which would cause delays in all Configuration Manager functions. To lower the risk of this happening, use MIF collection only when it is absolutely necessary. Later in the chapter, you'll see how to change the location of MIF files from the default.

More on NOIDMIF Files

NOIDMIF files are the standard MIF files that are used in Configuration Manager hardware inventory. NOIDMIF files do not contain a unique identifier for the data they contain, and hardware inventory automatically associates the NOIDMIF information with the client that it was found on. NOIDMIF files are not sent to the site server during a client hardware inventory cycle, but their data is added to the client inventory report itself.

If the classes in the NOIDMIF file don't exist in the Configuration Manager database, the new inventory class tables are created in the Configuration Manager site database to store the new inventory information. As long as the NOIDMIF file is present on the client, the inventoried data from the NOIDMIF file will be updated in the Configuration Manager database. If the NOIDMIF file is removed, all the classes and properties relating to it are removed from the inventory of that client in the database. For NOIDMIF information to be pulled from a client, the NOIDMIF file must be stored here: `%windir%\ccm\inventory\Noidmifs`.

More on IDMIF Files

IDMIF files are custom MIF files that contain a unique ID and are not attached to the client that they are collected from. IDMIF files can be used to collect inventory data about devices that are

not Configuration Manager clients, such as a shared network printer, an external hard drive, a copy machine, or other equipment that may not be attached to a client computer.

When you enable the IDMIF collection on your Configuration Manager site, IDMIF files are collected only if they are within the size limit that you set in the Hardware Inventory Client Agent properties. Depending on the maximum custom MIF size that you set for each site, IDMIF collection may cause increased network bandwidth usage during client inventory, which you should consider before you enable IDMIF collection.

Differences between NOIDMIF and IDMIF Files

IDMIF files are in most ways the same as NOIDMIF files. Both types have key properties that must be unique. Any class that has more than one instance must at least have one key property defined, or instances will overwrite previous instances. They differ in the following ways:

- IDMIF files must have a delta header that lists the architecture and a unique ID. NOIDMIF files are given a delta header automatically when processed by the client.
- IDMIF files must have a top-level group with the same class as the architecture being added or changed, and the class must have at least one property.
- Removing an IDMIF file from a client doesn't cause any data to be deleted from the Configuration Manager database.
- IDMIF files aren't added to a client's inventory, and the files themselves are sent across the network to be processed by a site server.

Collecting Software Inventory

When you enable Software Inventory in Configuration Manager, the software inventory process collects software inventory data directly from files by gathering data from the file's header information. Unknown files (files that don't have any detailed information in their file headers) can also be inventoried. You can also have Configuration Manager actually collect files you configure under a certain size. Both software inventory and collected file information can be viewed in Resource Explorer, which we will discuss later in the chapter.

You can also inventory encrypted and compressed files. This may cause Software Inventory to run more slowly because of the extra processing imposed on the client computer. When you inventory an encrypted file, an unencrypted copy of the file must be made so its information can be scanned. If antivirus software is running at the same time, it may show that the software inventory process is opening the files that are being scanned and then scanning them again to make sure they aren't infected by a virus.

Software Inventory can use a considerable amount of network capacity (especially if collecting files) and also increase disk activity along with CPU usage locally on the computer while running, depending on the number of Configuration Manager clients, how frequently you schedule Software Inventory, and the size of the files you collect (if any). If you think that Software Inventory will cause problems with your network, schedule it to run after business hours. Figure 11.2 shows the default Software Inventory settings; notice that no file types are selected by default.

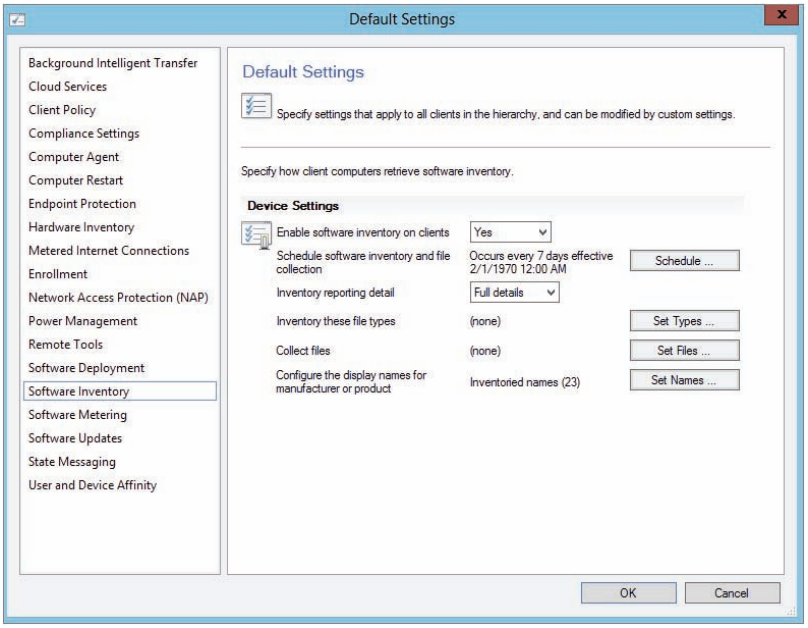


Figure 11.2 Default Software Inventory settings

More about File Collection

When a file is selected for collection, the Software Inventory Client Agent will search for that file when a software inventory scan runs on each client in the Configuration Management site. If the Software Inventory Client Agent finds a file that should be collected, then the file is attached to the inventory report and sent to the site server.

The site server keeps the five most recently changed versions of the collected files and stores them in the *<Configuration Manager installation directory>*\Inboxes\Sinv.box\Filecol directory. If a file has not changed since the last software inventory was collected, the file will not be collected again. Files larger than 20 MB are not collected by Configuration Manager software inventory file collection even if they are defined in the file collection settings.

This feature of Configuration Manager can greatly affect network bandwidth, as well as cause other problems, and is not typically utilized.

Display Names for Software Inventoried Products

During a software inventory cycle, the Configuration Manager 2012 software inventory process gets information from the file headers of files installed on clients. That information, including the names of the companies that made the files and the names of the files (or software products) themselves, is also inventoried. After the data is collected, you can view the information with Resource Explorer.

Because company and product names are retrieved from the file header information, any mismatches in the way these names are entered in the header information will also appear in

the Configuration Manager database. These mismatches make it difficult to read and query against software inventory information since the data will appear to be under multiple company or software product names instead of a single name.

To help with this issue, you can set display names for inventoried products on the Inventoried Names tab of the Software Inventory Client Agent tab. For example, you can do the following:

1. Change variations of a company name to a single display name.
2. Refresh the view of software inventory in Resource Explorer.

You will see the changes. You will also see them when you make and run queries.

Doing this doesn't actually change the names in the file header information of the files installed on clients; it changes the names in the Configuration Manager site database.

Using Resource Explorer to View Inventory

When hardware and software inventory is collected from clients, it can be viewed in Resource Explorer. When you start Resource Explorer, a new console opens, as shown in Figure 11.3.

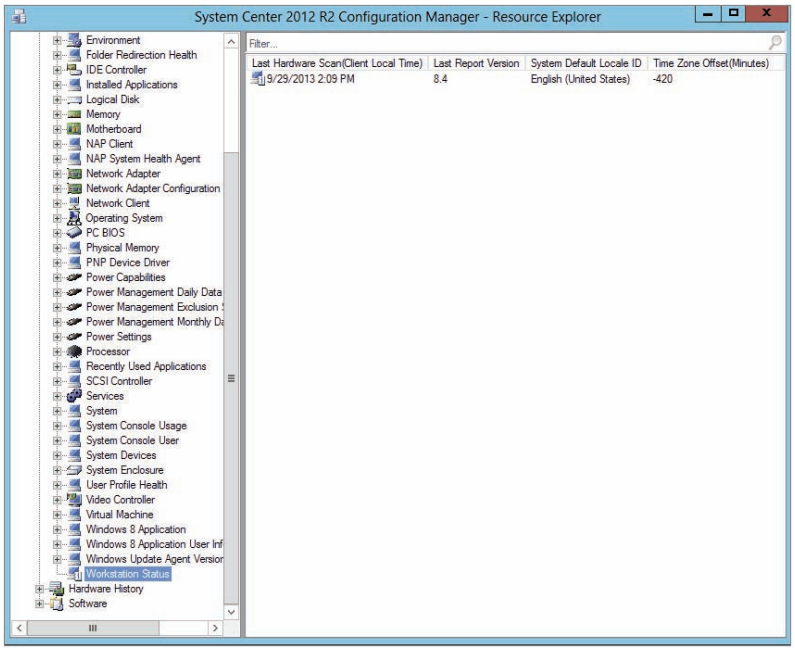


FIGURE 11.3 Resource Explorer

This displays the information collected from clients by hardware inventory and software inventory. The contents of the Resource Explorer details pane on the right will vary depending on what node is selected on the left pane in the console tree. You can use Resource Explorer to view client hardware, hardware history, and software inventory.

If a resource is a Configuration Manager client and if you are collecting hardware inventory at your site, the information displayed for that resource will be a list of the hardware installed on the client and other details. If you are collecting software inventory, then you will see a list of installed software on the client. If the resource isn't a Configuration Manager client, then no information will be displayed, since no inventory will be collected from that client.

You can start Resource Explorer to view a single client's inventory from the Configuration Manager console.

To open Resource Explorer from the Configuration Manager console, follow these steps:

1. In the Configuration Manager console, select Assets and Compliance ➢ Overview ➢ Devices.
2. Find the client that you want to view.
3. Once you have selected the client you want, click Start ➢ Resource Explorer on the ribbon.

Scheduling Inventory

The hardware inventory and software inventory processes each collect inventory according to a schedule that is set in the client settings. Table 11.1 gives a simple rundown of scheduling options for each inventory process.

TABLE 11.1: Inventory scheduling options

TYPE	DESCRIPTION
Simple schedule	An interval between inventory cycles, such as every day
Custom schedule	A start time and an interval for inventory collection, such as every Monday or the first Tuesday of every month at a specified hour of the day

By default, both hardware and software inventory schedules are set to run every seven days. If a client is not running when an inventory is schedule to run, it will run the inventory the next time the client is started.

The simple schedule doesn't give you as much flexibility as custom scheduling does; however, the simple schedule usually causes less network traffic because the time interval between each client's inventory cycle is based on the time that the Configuration Manager client was installed and when the first policies are retrieved, for every client. When you use a custom schedule, all the clients will begin inventory cycles at exactly the same time.

Since software inventory is more resource intensive on clients than hardware inventory, you might consider not running software inventory as often as you do hardware inventory, depending on your organization's needs. For example, if your organization has locked down user rights on workstations, then the software that is installed on them should not change frequently, so you can set software inventory cycles for every few days or once a week.

When you change an inventory collection schedule on the Configuration Manager site server, this will update the client computer policies downloaded and compiled by clients according to

their regular client policy polling interval. When the client inventory agent detects a change in schedule, it will make a delta inventory file. The next inventory cycle will run according to the new schedule.

Configuration Manager also keeps historical inventory records for the number of days set in the Delete Aged Inventory History site maintenance task, which has a default setting of 90 days.

Scheduling Inventory

Even if all installations are unique, it is often considered best practice to have a daily hardware inventory schedule and a weekly software inventory schedule. For servers it is often considered good practice to have a custom schedule for both inventory processes. That way you can schedule when inventory will run and not put a load on the hardware during peak hours.

Configuring Inventory

Now that we have discussed the inventory process, its components, and its capabilities, you are ready to configure the inventory function to fit your company's needs.

Configuring Hardware Inventory for a Configuration Manager Site

Before you configure Hardware Inventory, you need to know what kind of information you are gathering. In essence you have three different scenarios, as explained in Table 11.2.

Table 11.2: Inventory scenarios

Scenario	How to Gather the Inventory
Data class already exists in the default client settings.	All you have to do is enable the class in either the default client settings or in custom client settings as explained later in this chapter.
Data class does not exist in the default client settings but exists locally in WMI on each client.	On the Central Administration Site, open the default client settings. Connect to a remote host containing the data class, and import the data class.
Data class does not exist in the default client settings or on any of the local clients.	On one of the clients add the information to WMI. On the Central Administration Site open the default client settings. Connect to a remote host containing the data class and import the data class.

Configuring the Default Hardware Inventory Client Settings

To configure the default hardware inventory, select Client Settings in the Administration workspace. Open the default client agent settings properties, select Hardware Inventory, and click Set Classes, as shown in Figure 11.4. You can configure the following properties:

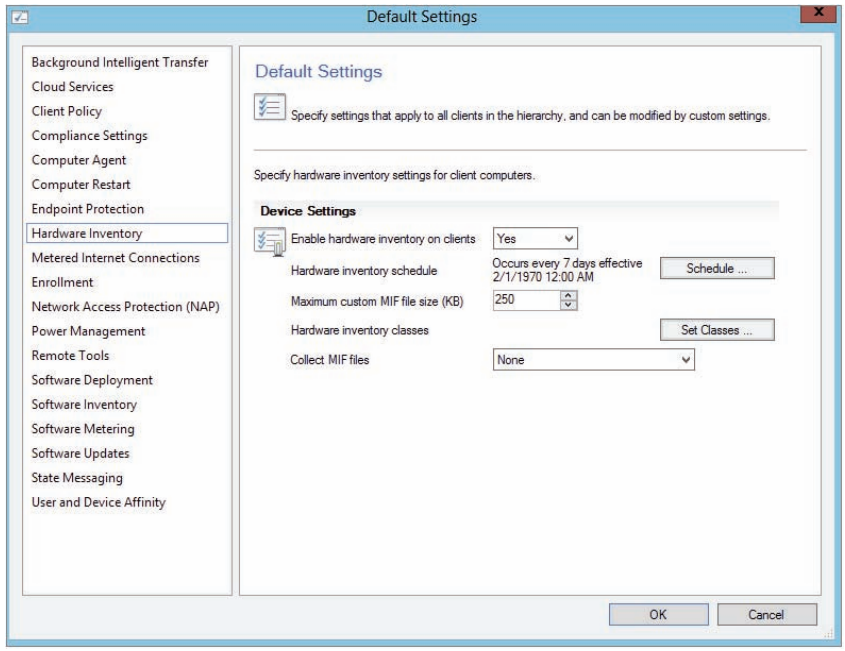


FIGURE 11.4 Configuring Hardware Inventory

Enable Hardware Inventory On Clients Configure this to True to enable (the default) or False to disable hardware inventory. Disabling hardware inventory is not recommended.

Hardware Inventory Schedule Click Schedule and select a simple schedule or define a custom schedule:

Simple Schedule This schedules hardware inventory to run at a single, specific interval for all clients that read the client settings. By default, this option is enabled and set for 7 days. For any other setting, use the Run Every field, and enter the number and type of time units (minutes, hours, days) in the simple schedule. This setting can be from 1 to 59 minutes, from 1 to 23 hours, or from 1 to 31 days.

Custom Schedule Click Customize to open the Custom Schedule dialog box and set the hardware inventory schedule. This gives you the ability to schedule the first start date and time for inventory to run on clients. Once the start time for inventory has passed, all future inventories will recur on the schedule that you set on all clients at the same time. The custom schedule can be set to run weekly, to run monthly, or to run on a custom interval, with the following criteria:

- Custom weekly schedules can run from 1 to 4 weeks on the day of the week you set.
- Custom monthly schedules can run from 1 to 12 months on either a specific day of the month from 1 to 31; the last day of each month; or the first, second, third, fourth, or last selected day of the week for each month.
- Custom schedules can also be set on a custom interval of either 1 to 31 days, 1 to 23 hours, or 1 to 59 minutes.

Collect MIF Files From the drop-down box select whether you want to collect IDMIF, NOIDMIF, both types, or none of them (default setting).

Maximum Custom MIF File Size (KB) This is the maximum size, in kilobytes, allowed for each custom MIF file that will be collected from a client during a hardware inventory cycle. You can set the size from 1 KB to 5,120 KB; the default value is 250 KB. If a custom MIF is larger than the maximum size, the Hardware Inventory Client Agent will move the IDMIF to the `\Badmifs` folder, and the IDMIF file will not be sent to the site server to be processed.

Collect IDMIF files Adds a new architecture and attributes and classes to the Configuration Manager database.

Collect NOIDMIF files Extends the hardware inventory by adding attributes and classes to existing architectures on a client. They are used to extend, or add, new information about existing Configuration Manager clients to the site database.

Changing the Default MIF Storage Location on a Client

You can change the MIF storage location after the client is installed by modifying the registry keys for the IDMIF and MOIDMIF files.

To change the default location for IDMIF files, follow these steps:

1. On the client for which you want to change the MIF location settings, select Start ➢ Run, type **`regedit`**, and then press Enter to start the Registry Editor.
2. Go to the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Configuration\Client Properties : IDMIF Directory`.
3. Right-click IDMIF Directory, and click Modify.
4. Enter the path to which you want to change; then click OK.
5. Close the Registry Editor.

To change the default storage location for NOIDMIF files, follow these steps:

1. On the client that you want to change the MIF location settings, select Start ➢ Run, type **`regedit`**, and then press Enter to start the Registry Editor.
2. Go to the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Configuration\Client Properties : NOIDMIF Directory`.
3. Right-click NOIDMIF Directory, and click Modify.
4. Enter the path to which you want to change; then click OK.
5. Close the Registry Editor.

Note that this procedure will change the MIF storage location on only the client that you worked on. If you want to make this a site-wide client change, you can use the remediation feature in Settings Management.



Real World Scenario

Configure Custom Hardware Inventory Changes for All Laptops

As the Configuration Manager administrator, you have been requested to ensure that portable battery information is inventoried for all laptops.

1. Open the Configuration Manager 2012 administrative console.
2. Select the Administration workspace and browse to Client Settings.
3. On the ribbon click Create Custom Client Device Settings.
4. Type **Hardware Settings for laptops** in the Name field.
5. From the list of custom settings, select Hardware Inventory.
6. In the left column, select Hardware Inventory and click Set Classes.
7. Find Portable Battery (Win32_Portable) and enable the data class.
8. Click OK.
9. Click OK to save the custom client settings.
10. Back in the administrative console, select the newly created custom settings and click Deploy on the ribbon.
11. Select the All Laptop device collection and click OK.

Extending Hardware Inventory

As described in Table 11.2, you can also customize Hardware Inventory to collect information that is not reported by default or add totally new information that you want to be collected that you configure yourself.

You can extend Hardware Inventory by inventorying additional WMI classes, additional WMI class attributes, registry keys, and other customizations to fit your company's needs. If you need to, you can also modify Hardware Inventory to reduce the amount of information reported by clients.

Before you start modifying the `configuration.mof` file, you should make sure you have a good idea of what you are doing and make backups of the file before you edit it. You should also consider performing the proposed changes in a Configuration Manager test lab so that you can effectively monitor the results of the changes without impacting the production environment.

There are a few resources available to help you with extending hardware inventory. For example, the article "How to Extend Hardware Inventory in Configuration Manager" discusses how to configure and extend the hardware inventory feature in Configuration Manager; see `http://technet.microsoft.com/en-us/library/gg712290.aspx`.

Providers Used in Hardware Inventory

When you extend hardware inventory that is collected by Configuration Manager clients, the `configuration.mof` file is modified to inventory client information by leveraging a registered inventory data provider. Providers used during client hardware inventory are listed at the top of the `configuration.mof` file and are registered on clients when they first get a computer policy, and then they compile the `configuration.mof` file after the Configuration Manager client is installed.

Extending Hardware Inventory Using the configuration.mof File

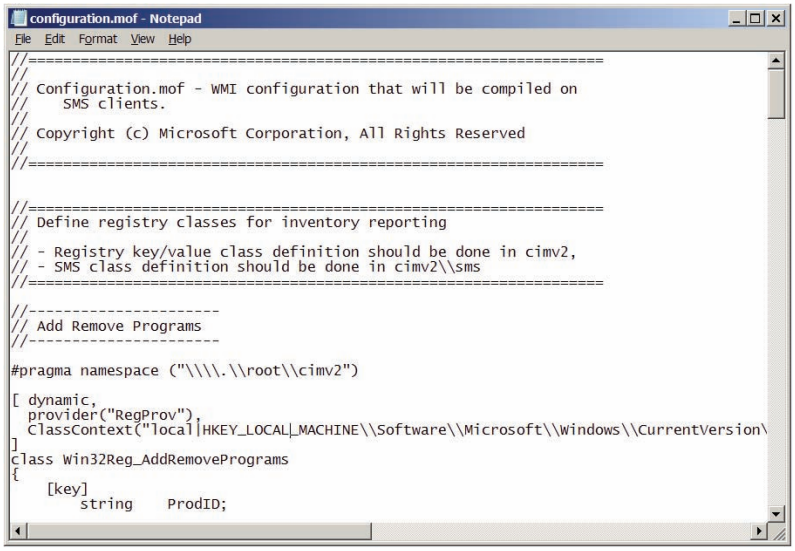
The `configuration.mof` file is used to modify data class information inventoried by clients with hardware inventory.

To modify the `configuration.mof` file, follow these steps:

1. Make a backup copy of the `configuration.mof` file, and put it in a safe location.
2. On the primary site server, go to the *<Configuration Manager install folder>*`/inboxes/clifiles.src/hinv` folder.
3. Using Notepad, open the `configuration.mof` file, and make any necessary changes.

   Figure 11.5 shows part of the `configuration.mof` file.

FIGURE 11.5
The `configuration.mof` file



4. Close the `configuration.mof` file, and save the changes.
5. Copy the `configuration.mof` file to the same location that is listed in step 2 and to all the primary sites in your hierarchy to propagate the changes to the other sites. Note that ConfigMgr does not copy this file for you; you must copy the file to the other primary site servers in your hierarchy in order to achieve consistent inventory results from your clients.

Extending Hardware Inventory Using the Default Client Settings

The default client settings are used to modify reporting class information inventoried by clients during hardware inventory. The default client settings contain a list of classes and attributes that relate to data classes stored in the WMI repository of Configuration Manager clients.

Classes and properties that have the reporting checkmark enabled are collected, and those without a checkmark are not. You must always modify the default classes in the default client settings at the Central Administration Site; you will not be able to enable or disable these settings in any custom client settings.

To modify the default client settings, follow these steps:

1. Navigate to the Administration workspace, under Overview select Client Settings, and open the Default Client Settings properties.
2. Select Hardware Inventory and click Set Classes.
3. Use the GUI to enable or disable any of the existing inventory data classes.
4. Choose OK to save the changes.
5. Close the Default Client Settings properties.

Configuring Software Inventory for a Configuration Manager Site

Software Inventory is enabled by default when you install Configuration Manager, but unlike previous versions, ConfigMgr 2012 will not inventory any files by default. In order to perform software inventory on files types, like files with an `.EXE` extension, you must configure the setting:

1. Navigate to the Administration workspace, under Overview select Client Settings, and open the Default Client Settings properties.
2. Select Software Inventory.

   The first thing you will see is the default settings, as shown in Figure 11.6.
3. Click Set Types.
4. Click the yellow starburst New icon to create a new entry.
5. Type **`*.exe`**, as shown in Figure 11.7, and click OK twice.

   This will search for EXE files on the entire hard disk, excluding the `Windows` folder and encrypted/compressed files. If you want to, you can specify which folders to include in the scanning; likewise, you can specify a filename instead of a file type. It is worth noting that as you add file types, you will extend the amount of time that software inventory will run on the client computers.

   Inventory Reporting Detail is by default set to Full Details. This will ensure that you gather information about the file regardless of whether the file has a product mentioned in the file header or not. Selecting Product Only will not gather information from unknown files.

   Collect Files allows you to copy a file from the client and store a copy on the site server. When you enable this feature, the site server will keep up to five versions of each file in *`<Configuration Manager installation directory>`*`\Inboxes\Sinv.box\Filecol`. Even though it sounds tempting to collect files, you should think twice before enabling this feature. It can generate a substantial amount of network traffic and cause your site server to run

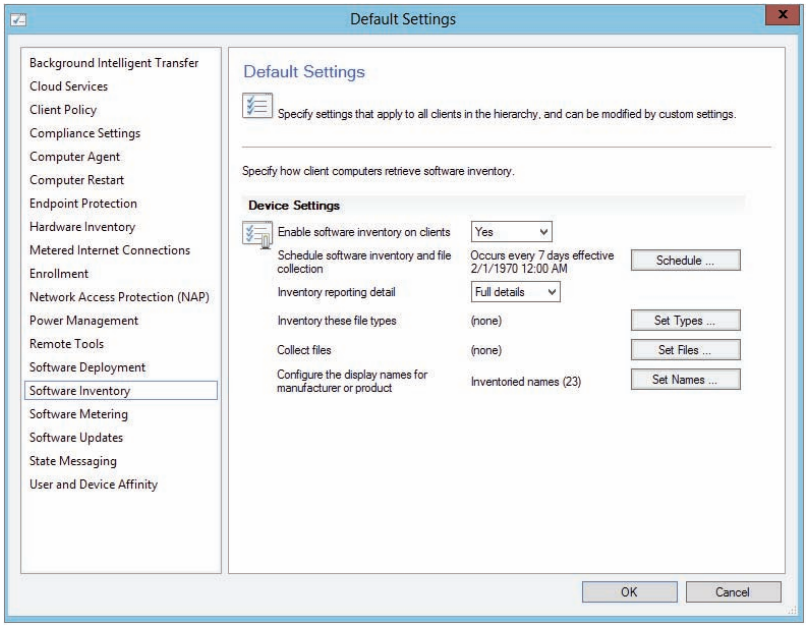


FIGURE 11.6
Default Software Inventory settings

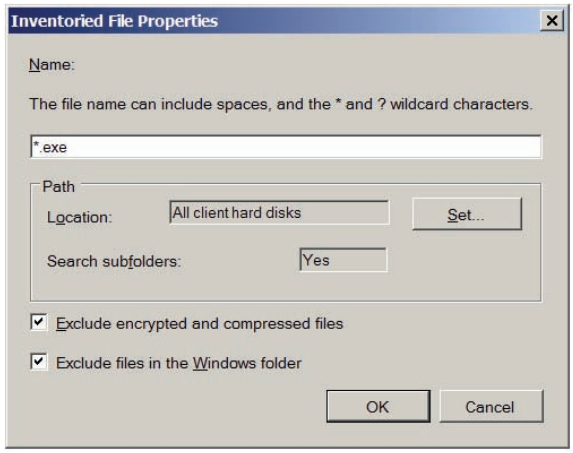


FIGURE 11.7
Scanning for EXE files

low on disk space. As shown in Figure 11.8, you can collect a single file or all files of a certain file type.

6. To specify a file, click the yellow starburst New icon, and type a filename or use a wildcard to specify a given type.

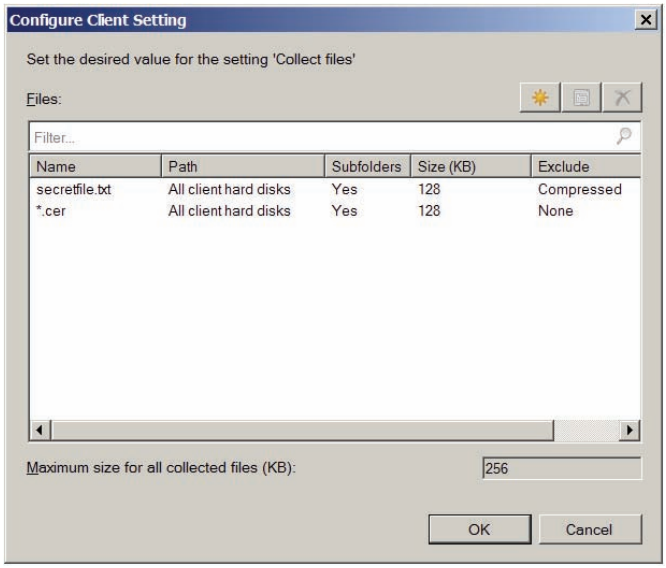


FIGURE 11.8
Collecting files

7. Click Set to narrow the search to a given location; this will speed up the process.

   Figure 11.9 shows how you can search for all `*.sus` files in the `%programfiles%\MySoftware` folder.

   Configuring the display names for manufacturer or product allows you to group files according to the correct vendor and application. As mentioned earlier in this chapter, the

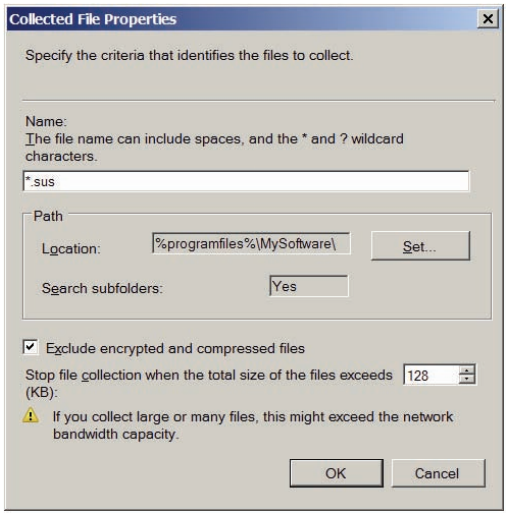


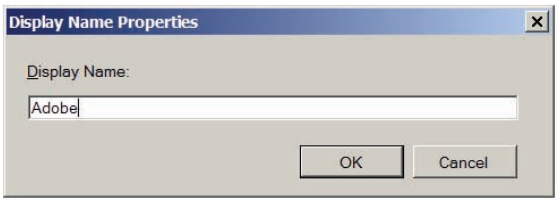
FIGURE 11.9
Specifying all `*.sus` files from a folder

names are derived from the file header, which often contains alternative ways to spell the manufacturer's name.

8. Click Set Names, and click the yellow starburst New icon to configure a new display name.

   Figure 11.10 shows a new display name for Adobe applications.

FIGURE 11.10
Configure a new display name.



9. Once the display name is created, select the display name and click the yellow starburst New icon to the right of Inventoried Names.

   When you specify an entry in the Inventoried Names section, you can use these wildcard variables:

%	Any string of zero or more characters
_ (underscore)	Any single character
[ ] (brackets)	Any single character within a range
[^]	Any single character *not* with a range

10. When you have typed a name, click OK.

    Figure 11.11 shows an example where all inventory names starting with "Adobe" will be grouped below the Adobe manufacturer.

Viewing Software Inventory Data

Software inventory information is often used in queries and reports. In the Configuration Manager administrative console, you can use Resource Explorer to view information from a single client (Figure 11.12). You will be able to read file information including File Name, File Path, File Size, File Version, and File Modified Date. The information is divided into four sections, as described in Table 11.3.

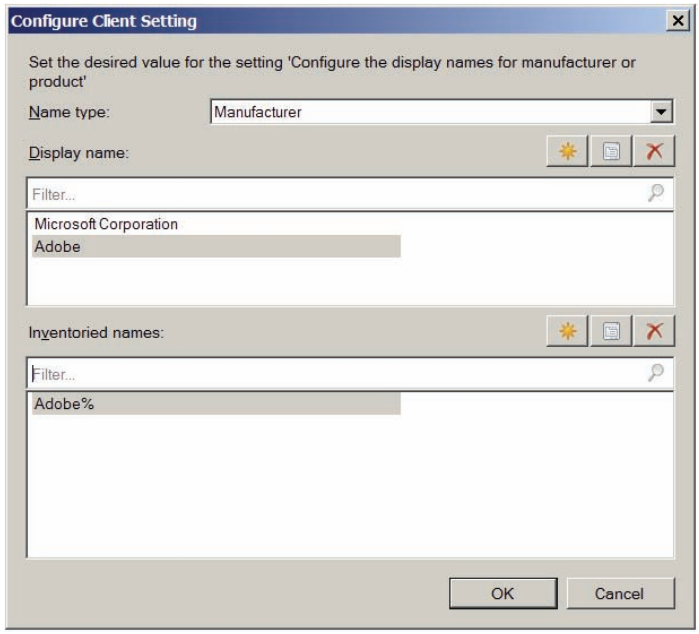


FIGURE 11.11
A custom display name

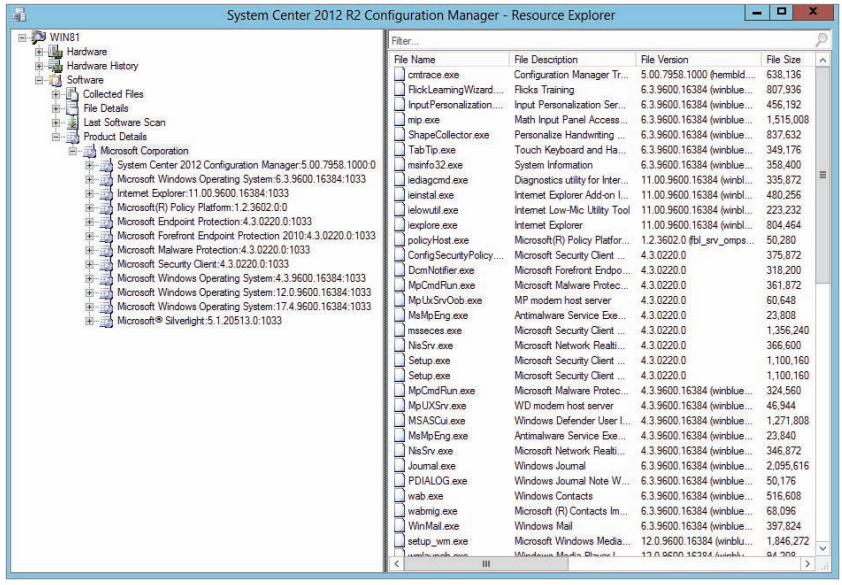


FIGURE 11.12
Software information in Resource Explorer

Table 11.3: Software information in Resource Explorer

Section	Information available
Collected Files	Lists all files collected from the client.
File Details	Lists all inventoried files that are not associated with any vendor.
Last Software Scan	Lists the last file collection and software inventory scanning data.
Products Details	Lists all inventoried files that are associated with a vendor. You can modify the list of vendors by customizing the display name in the Software Inventory Client Settings.

Miscellaneous Inventory Configurations and Options

The following sections cover some configuration options for inventory that don't neatly fit into other categories.

Encrypting Client Inventory Reports

Configuration Manager can be configured to sign and encrypt data sent between the client and the management point. To enhance security for inventory, you can enable inventory encryption.

To enable inventory encryption, follow these steps:

1. In the Configuration Manager console, select the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites.
2. Right-click the site and click Properties.
3. Click the Signing And Encryption tab.
4. Select Use Encryption.
5. Click OK to finish.

Excluding Files from Software Inventory

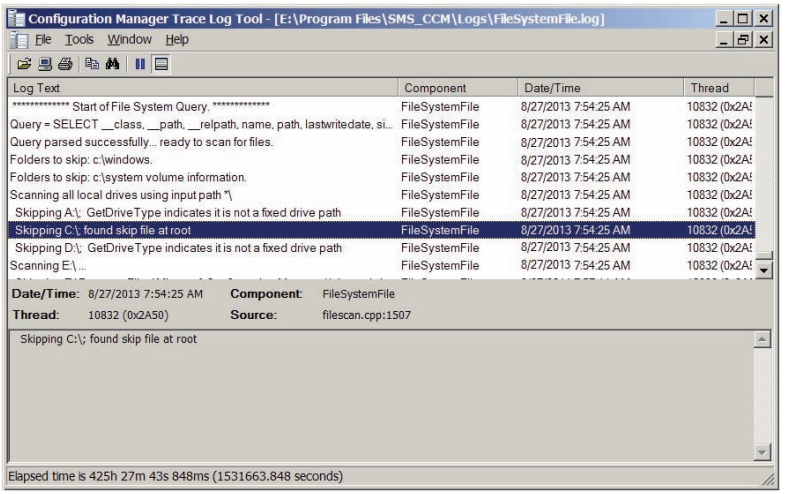
To exclude folders or entire drives from the software inventory process, create a file called `skpswi.dat` and save it to the root of the area (and subfolders) you want to exclude. You can skip the entire `C:` partition by storing the file in `C:\` or a folder (and subfolders) by saving the file in the root of the folder.

You can ensure that folders and drivers are excluded by reading the `FileSystemFile.log` file on the client. Figure 11.13 shows how you can verify that the `skpswi.dat` file is working.

To exclude files from software inventory, follow these steps:

1. Using Notepad, make an empty file named `skpswi.dat`.
2. Right-click that file, and click Properties.

FIGURE 11.13
FileSystemFile.log



3. In the file properties for `skpswi.dat`, select the Hidden attribute.
4. Place the `skpswi.dat` file at the root of the drive or folder where you don't want to collect software inventory.

Monitoring the File and Size Being Sent to the Management Point

One of the questions you often hear before enabling any inventory process is how much network utilization is generated by running this process? The Configuration Manager client will send Heartbeat Discovery data, hardware inventory data, and software inventory data on a regular basis. The three files generated by each of these processes will be temporarily stored in `%systemroot%\ccm\inventory\temp\` before being sent to the management point. After files are sent to the management point, they will automatically be deleted from the `temp` folder. You can create a file called `archive_reports.sms`, discussed next, and save it to the same folder. This will prevent the Configuration Manager client from deleting the XML files after they are sent to the management point.

Figure 11.14 shows three files generated: one for hardware inventory, one for software inventory, and one for Heartbeat Discovery.

To prevent XML files from being deleted, follow these steps:

1. Using Notepad, create an empty file named `archive_reports.sms` (make sure that it's not a `.txt` file).
2. Save the file in the `%systemroot%\ccm\inventory\temp\` folder.
3. Initiate a hardware, software, and/or discovery inventory cycle on the client, and monitor the `%systemroot%\ccm\inventory\temp\` folder.

   You should be able to see one XML file for each process that contains data.

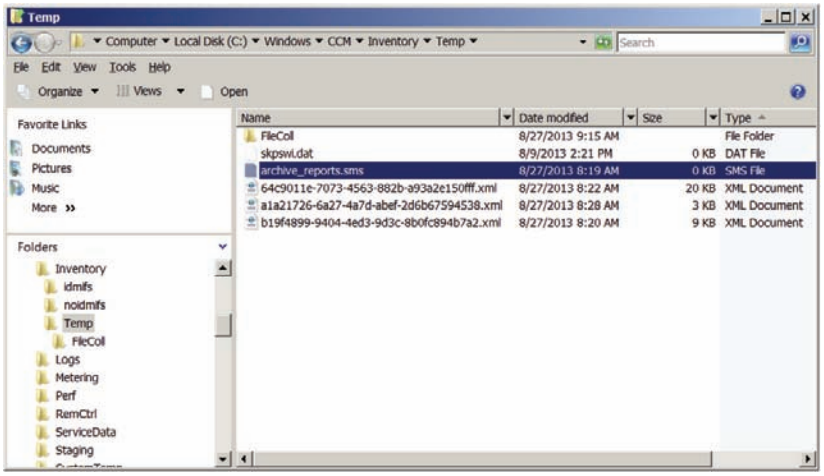


FIGURE 11.14
Files generated by the inventory and discovery processes

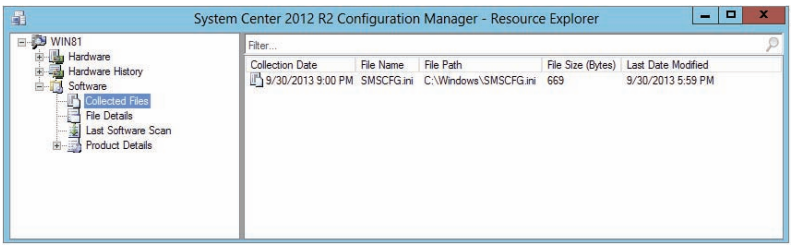


FIGURE 11.15
Reading a collected file in Resource Explorer

4. Remember to delete the `archive_reports.sms` file from the client once you have enough information to estimate the average file size for each of the three processes. Note that the first hardware and software inventories will be larger than subsequent inventory files, whereas the heartbeat discovery file should always be about the same size.

Viewing Collected Files

You can view collected files by opening the `<:\>Program Files\Microsoft Configuration Manager\inboxes\sinv.box\FileCol\` folder on the site server or through Resource Explorer. Using Resource Explorer is by far the best method because it will link the collected files and computer together. As shown in Figure 11.15, you can open and read each collected file.

To view the collected files of a particular client, follow these steps:

1. In the Configuration Manager console, select the Assets and Compliance workspace ➢ Overview ➢ Devices.
2. In the Search area of the ribbon, type the name of the client you wish to find and click Search.

3. Once you have found the client you want, right-click it.
4. Then click Start ➢ Start Resource Explorer.
5. In the left pane, select Software ➢ Collected Files.

   You will see a list of all the files that have been collected from that client in the right pane.
6. To view a file, you have two options:
   - Right-click a file, and select View File.
   - Right-click a file, and select Save.

Troubleshooting Inventory

The following sections cover some basic information that will help you troubleshoot specific problems. In order to troubleshoot and fully understand what's going on behind the scenes, you need to have information about the log files in the process.

Hardware Inventory

When you troubleshoot hardware inventory, you need to know how data travels from the client to the SQL database. Inventory data will be sent from the client to the management point and then to the site server before being added to the database.

Client-Side Processing

All client-side hardware inventory processes are recorded in the `InventoryAgent.log` file. The log file will contain several lines that are important for you to understand.

The following line tells you what kind of inventory report will be sent from the client to the management point. It can be a full, delta, or resync report.

```
Inventory: Action=Hardware ReportType=Delta
```

The following line queries for data:

```
Collection: Namespace = \\localhost\root\Microsoft\appvirt\client; Query = SELECT
__CLASS, __PATH, __RELPATH, LastLaunchOnSystem, Name, PackageGUID, Version FROM
Application; Timeout = 600 secs
```

The following line gives information about the number of classes that the client is searching for and the number of classes found. The information in this line is worth checking whenever you make changes to the data classes. When you enable an extra data class, the last number should increase by one.

```
Collection: 55/64 inventory data items successfully inventoried.
```

The following line basically informs you that the client-side processing has completed successfully and information has been sent to the management point.

```
Inventory: Successfully sent report. Destination:mp:MP_HinvEndpoint, ID:
{D886D5C8-59E4-4C9C-B9CD-08D7DA40BA20}, Timeout: 80640 minutes MsgMode: Signed,
Not Encrypted
```

Management Point Processing

At the management point the client data will be converted from an XML file to an MIF file and sent to the site server. You can monitor the process by reading the `MP_HINV.log` file.

Site Server Processing

At the site server the client data will be added to the SQL database by the Inventory Data Loader process. In the `Dataldr.log` file you will see entries similar to these:

```
Thread: 10368 will use GUID GUID:1E8A9DD4-C572-48F9-BEDB-B33D8E0F07F4
SMS_INVENTORY_DATA_LOADER   8/27/2013 11:34:04 AM   10368 (0x2880)
Processing Inventory for Machine: DC1   Version 1.7  Generated: 08/27/2013
11:33:27   SMS_INVENTORY_DATA_LOADER   8/27/2013 11:34:04 AM   10368 (0x2880)
Begin transaction: Machine=DC1(GUID:1E8A9DD4-C572-48F9-BEDB-B33D8E0F07F4)
SMS_INVENTORY_DATA_LOADER   8/27/2013 11:34:04 AM   10368 (0x2880)
Commit transaction: Machine=DC1(GUID:1E8A9DD4-C572-48F9-BEDB-B33D8E0F07F4)
SMS_INVENTORY_DATA_LOADER   8/27/2013 11:34:04 AM   10368 (0x2880)
Done: Machine=DC1(GUID:1E8A9DD4-C572-48F9-BEDB-B33D8E0F07F4) code=0 (20 stored
procs in XH3JZIA70.MIF)   SMS_INVENTORY_DATA_LOADER   8/27/2013 11:34:04 AM
10368 (0x2880)
```

The MIF file is added to the SQL database from

```
<:>\Program Files\Microsoft Configuration Manager\inboxes\auth\dataldr.box\
Process
```

If you see a large number of MIF files in one of the `dataldr.box` folders, it's normally a clear indication of a backlog.

When Clients Are Deleted from the Database but Not Uninstalled

A commonly seen issue occurs when an administrator accidently deletes all client computers from a collection. This will remove client data from the database, but the Configuration Manager Client Agent running on those systems is not aware of that action. In the following sequence you can see that the client is still sending delta inventory information to the site server, but since the site server does not have any existing records, it will not be able to process that delta data and asks the client to perform a resync.

In the `InventoryAgent.log` file on the client, notice that the first report type is delta.

```
<![LOG[Inventory: Action=Hardware ReportType=Delta]LOG]!><time="12:38:31.453-120"
date="08-27-2013" component="InventoryAgent" context="" type=""1" thread="212"
file="agentstate.cpp:1563">
```

The data loader component receives the delta information and tries to add it to an existing record in the database. The record does not exist in the database, which is why the MIF file is discarded and moved to the `Badmifs` folder. Furthermore, the data loader component will initiate a resync, which instructs the client to send up a full inventory report.

```
ERROR - attempt to update non-existent row. Invalid command:  exec
dbo.pWorkstationStatus_DATA 1,16777222,'08/27/2013 12:49:49',1,'8/27/2013
12:49:42',N'4294967305',1033,120  $$<SMS_INVENTORY_DATA_LOADER><08-27-2013
12:49:49.740-120><thread=2720 (0xAA0)>
Rollback transaction: Machine=DC1(GUID:1E8A9DD4-C572-48F9-BEDB-B33D8E0F07F4)
$$<SMS_INVENTORY_DATA_LOADER><08-27-2013 12:49:49.744-120><thread=2720 (0xAA0)>
Remote client hardware inventory resync generated for client GUID:1E8A9DD4-
C572-48F9-BEDB-B33D8E0F07F4; update/insert result = 2  $$<SMS_INVENTORY_DATA_
LOADER><08-27-2013 12:49:49.825-120><thread=2720 (0xAA0)>
~Send resync command to local site for machine GUID:1E8A9DD4-C572-
48F9-BEDB-B33D8E0F07F4.  $$<SMS_INVENTORY_DATA_LOADER><08-27-2013
12:49:49.830-120><thread=2720 (0xAA0)>
STATMSG: ID=2722 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_INVENTORY_DATA_
LOADER" SYS=SCCM4.sccmlab.local SITE=RC1 PID=9052 TID=2720 GMTDATE=Sat
Aug 27 10:49:49.833 2013 ISTR0="DC1" ISTR1="" ISTR2="" ISTR3="" ISTR4=""
ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0  $$<SMS_INVENTORY_DATA_
LOADER><08-27-2013 12:49:49.835-120><thread=2720 (0xAA0)>
~Cannot process MIF XHIJ3F4L2.MIF, moving it to e:\Program Files\Microsoft
Configuration Manager\inboxes\auth\dataldr.box\BADMIFS\44p7g21x.MIF  $$<SMS_
INVENTORY_DATA_LOADER><08-27-2013 12:49:49.843-120><thread=2720 (0xAA0)>
```

On the client, the next hardware inventory will send a full hardware report to the management point. Notice the `ReportType=Resync` notation:

```
![LOG[Inventory: Opening store for action {00000000-0000-0000-0000-000000000001}
...]LOG]!><time="13:03:21.391-120" date="08-27-2013" component="InventoryAgent"
context="" type="1" thread="2668" file="datastore.cpp:176">
<![LOG[Inventory: Action=Hardware ReportType=ReSync]
LOG]!><time="13:03:37.734-120" date="08-27-2013" component="InventoryAgent"
context="" type="1" thread="2668" file="agentstate.cpp:1563">
```

Once the resync report is processed, the client will be added to the database and will show up in the Configuration Manager administrative console.

When Clients Try to Inventory Data Classes That Don't Exist

As we have already discussed, the Hardware Inventory Client Agent gets information about a computer's hardware from the WMI data classes. Sometimes not all of the WMI data classes that Configuration Manager is set up to inventory are present on a client.

Clients with different operating systems are a good example. The default client settings are configured to inventory certain new WMI classes in Windows 2008 R2 that aren't available on other operating systems. The hardware inventory process will still try to inventory those classes on a Windows 7 or Windows Vista client since they also read the settings in the default client settings.

When a client tries to inventory a class that doesn't exist, you will see an entry only in the `InventoryAgent.log` file, because no status message will be sent to the site server. If you need to figure out whether a client is trying to inventory nonexistent data classes, you will see entries similar to `Collection: Class "<Class Name>" does not exist` in the `InventoryAgent.log` file.

Software Metering in Configuration Manager 2012

Software Metering is used to track usage of administrator-defined applications using software-metering rules. It is not used to prevent users from running an application (this is a job for the Software Restriction Group Policy). By default Configuration Manager will automatically create disabled software metering rules based on the recently used inventory data. Often you will find yourself disabling the feature and creating your own software metering rules.

Overview of Software Metering

Software Metering in Configuration Manager 2012 allows you to monitor and collect information about software usage on Configuration Manager clients. The information collected is based on the software metering rules that can be configured in the Configuration Manager console or created automatically based on usage data collected by inventory.

The Software Metering Client Agent on each client evaluates these rules, collects the requested data, and then reports it to the Configuration Manager database. The software metering process will continue to collect usage data even if it can't connect to its management point and will send the collected data on to the site server after it connects to the network. By default clients will send the software metering usage report every seven days.

Software metering data is held on the site server until it is summarized. The summarization schedule is defined in the Site Maintenance tasks for the site. By default the process will begin every night at 00:00.

You will be able to see the software metering data in the reports once the software metering report data has been received on the site server and summarized. By default this process can take up to eight days from client activity to seeing information in reports. This might sound like a long delay, but often you will only use the reports once a month or so when evaluating licenses. Combined with software inventory, software metering gives administrators a powerful tool to help answer questions that come up in every IT organization. Examples of these questions include the following:

- What is the relationship between how many instances of a software program are installed on clients and how many actually use that software?
- Do you need to buy more licenses when renewing your license agreement with a software vendor?
- What users are still using an obsolete program?

Configuring Software Metering

The Software Metering feature is enabled by default when you install Configuration Manager. You can enabled or disable the feature by editing the default Client Agent settings or creating a custom client setting.

Configuring the Software Metering Feature

Take these steps to configure the Software Metering feature:

1. Navigate to the Administration workspace, under Overview select Client Settings, and open the Default Client Settings properties.
2. Select Software Metering, and notice the default setting, as shown in Figure 11.16.

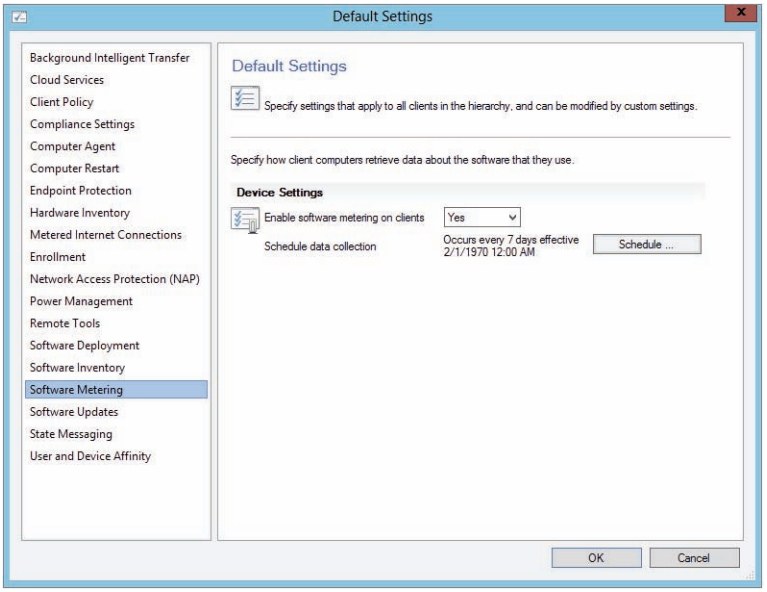


FIGURE 11.16
Default Software Metering settings

By default, Enable Software Metering On Clients is set to Yes.

3. To disable the feature, select No in the drop-down box.

   Schedule Data Collection defines how often the Configuration Manager client will send software metering data from WMI to the site server.

CONFIGURING AUTOMATIC SOFTWARE METERING RULE GENERATION

As discussed earlier in the chapter, Configuration Manager will automatically create disabled software metering rules based on recently gathered inventory data. You can configure or disable the feature from the Assets And Compliance workspace.

To configure automatic rule generation, follow these steps:

1. Navigate to the Assets and Compliance workspace, under Overview select Software Metering, and click Software Metering Properties on the ribbon.

   This opens the Software Metering Properties dialog box, as shown in Figure 11.17.

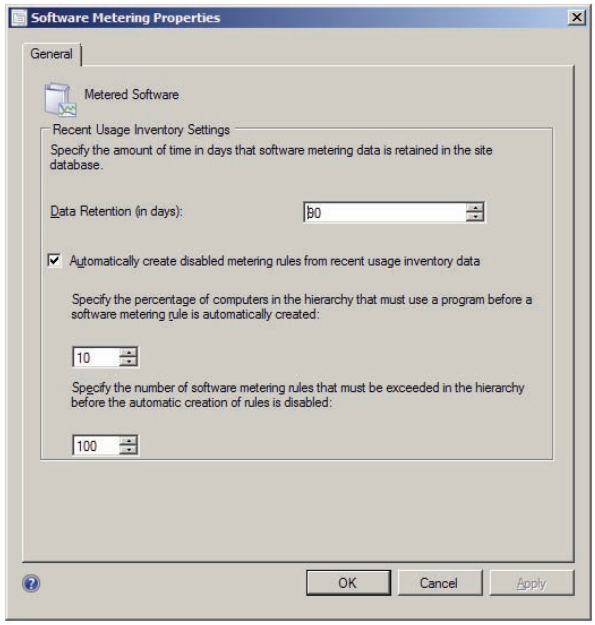


FIGURE 11.17
Software Metering Properties dialog box

2. You can set the following options:
   - You can specify the amount of time in Data Retention (In Days) that data generated by software rules will be held in the site database. The default setting is 90 days.
   - You can select the Automatically Create Disabled Metering Rules From Recent Usage Inventory Data check box.
   - You can set the percentage of computers in a Configuration Manager site that must use an executable before a software metering rule for that executable is automatically created. The default setting is 10 percent.
   - You can set the maximum number of rules that software metering will automatically generate. The default setting is 100 rules.
3. When you have finished setting these options, click OK.

Enabling and Disabling Software Metering Rules

You don't have to delete a rule if you don't want to use it; instead, you can enable it or disable it as needed if you want to keep it.

To enable or disable a software metering rule, follow these steps. Figure 11.18 shows automatically generated software metering rules in the Configuration Manager console.

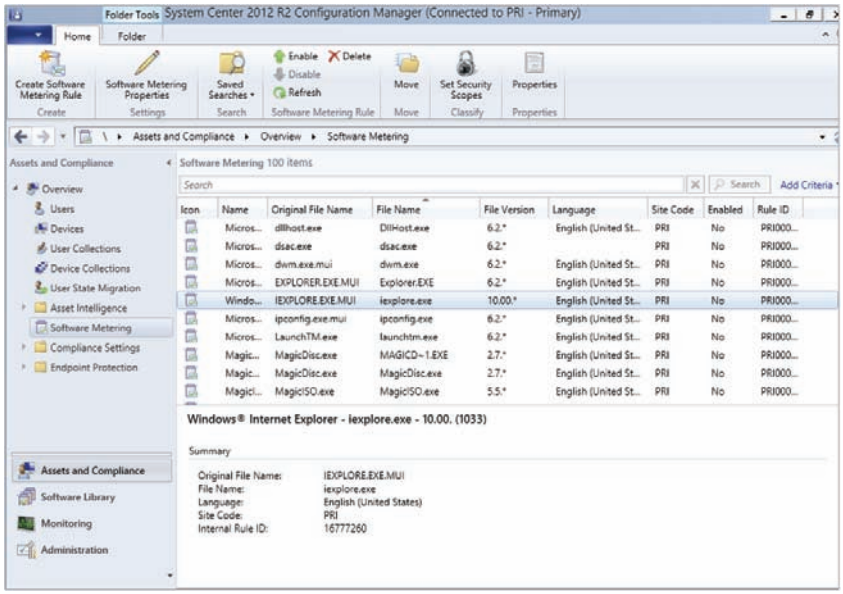


FIGURE 11.18 Software Metering node with software metering rules

1. Navigate to the Assets and Compliance workspace, and under Overview select Software Metering.
2. Right-click one or more rules that you want to configure, and then click either Enable or Disable.

   The option that is available will depend on what state the rule is already in.

ADDING A SOFTWARE METERING RULE

If the automatically generated rules aren't what you need, then you can manually make your own to meet your organization's needs. To make your own software metering rules, follow these steps:

1. Navigate to the Assets and Compliance workspace, and under Overview select Software Metering.
2. Click Create Software Metering Rule on the ribbon.

   This opens the General page of the Create Software Metering Rule Wizard, shown in Figure 11.19.

   This page has the following options:

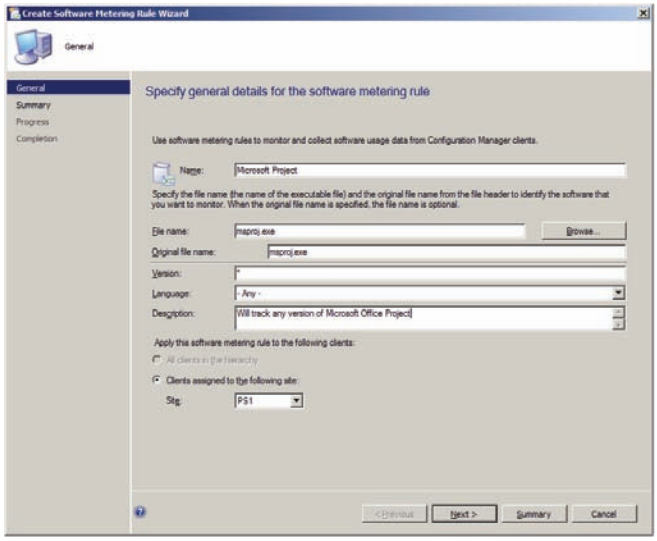


FIGURE 11.19
General page of the Create Software Metering Rule Wizard

Name The name of the software metering rule, which should be unique. You can have rules with the same name, as long as the filenames are different. This way you can track suites of applications like the Adobe Creative Suite or Microsoft Office.

File Name The name of the executable file you want to meter. You can click Browse to display the Open dialog box, where you can select the file that you want to meter. You can manually type in this filename, but when you do that, no checks are made to determine whether the file exists or whether it contains the needed file header information. For the best results, always use the Browse button if possible. Wildcard characters can't be used in this field, and selecting the Original File Name field is optional.

Original File Name The name of the executable file that you want to meter. This name is matched to the information in the file header, not the filename itself, so you still meter it if the file is renamed. Wildcard characters can't be used in this field, and selecting the File Name field is optional.

Version The version of the executable file that you want to meter. If you use the Browse button to select your file, this field will be filled out automatically from the file's header information (as shown in Figure 11.18). You can use the wildcard character (*) to represent any string of characters or the wildcard character (?) to represent any single character. If you want to meter all versions of the file, you can use the default value (*).

Language The language of the file that you want to meter. The default value is English (United States). If you use the Browse button to select your file, then this is filled out automatically from the file's header information. If you want to meter all language versions of this file, then select Any from the drop-down list.

Description A description that you want for the rule. This is an optional field.

Apply This Software Metering Rule To The Following Clients Your options are All Clients In The Hierarchy or Clients Assigned To The Following Site.

3. Fill in the information and click Next.
4. Review the information on the Summary page and click Next.
5. Click Close.

   The rule is now created and will be downloaded to clients during the next machine policy cycle.

Deleting Software Metering Rules

When you delete a software metering rule, the change will be downloaded to clients during their next policy polling interval, just like when you create rules.

To delete a software metering rule, follow these steps:

1. Navigate to the Assets and Compliance workspace, and under Overview select Software Metering.
2. Find the metering rule that you want to delete, right-click it, and click Delete.

   You will then see a Confirm Object Delete dialog box.
3. If you are sure that you want to delete this rule, then click Yes.

Software Metering Maintenance Tasks

Depending on how you configure software metering, you could end up with a lot of data collected in the Configuration Manager database. To help you manage that data, several maintenance tasks are included in the Configuration Manager console. There are four tasks in total in two categories—two tasks for deleting aged software metering data and two tasks for summarizing software metering data. All of these tasks are enabled by default.

To find them in the Configuration Manager console, navigate to the Administration workspace and under Overview choose Site Configuration ➢ Sites. From the ribbon click Site Maintenance.

Figure 11.20 shows the software metering Site Maintenance settings. To edit, just double-click the task you want to configure.

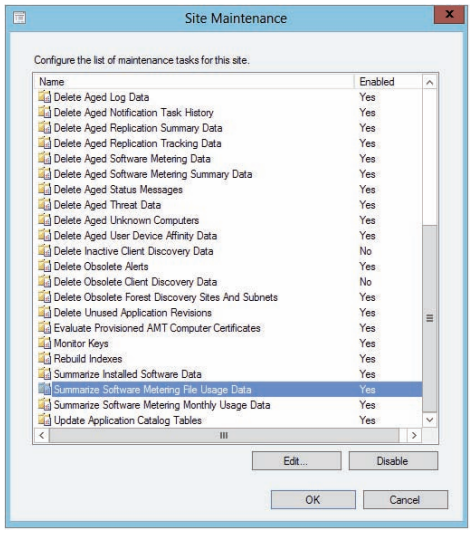


Figure 11.20
Software metering maintenance tasks

These tasks summarize software metering usage data to compress the amount that is stored in the Configuration Manager database. Summarization runs daily by default and will run only against data that is at least 12 hours old. This is required for all software metering reports to produce any meaningful data. To get an idea of what is in the most current set of summarized data, you have to know when that last summarization took place.

The Software Metering Summarization Progress report, as shown in Figure 11.21, will provide you with information about the last summarization process.

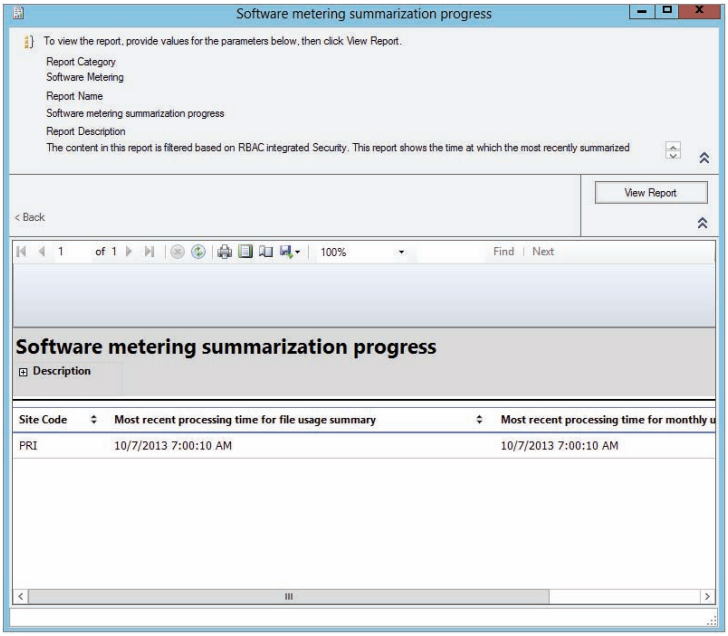


FIGURE 11.21 Software Metering Summarization Progress report

The Summarize Software Metering File Usage Data task summarizes software metering file usage data from several records into one record. This record gives information about the program name, version, language, and number of distinct users over intervals of 15 minutes to 1 hour. This process compresses and optimizes the amount of data stored in the Configuration Manager database.

For every hour and every 15-minute time frame within the hour, this task will calculate the total number of distinct user/computer combinations that are running the programs that are being metered. Within 15-minute intervals, this will give an approximate number of concurrent users of a metered program.

When software summary data is sent up the Configuration Manager hierarchy, data from each site is kept separate from the data from the other sites. When the data reaches a parent site, each record is marked with the site code of the site it came from.

The Summarize Software Metering Monthly Usage Data task summarizes detailed software metering usage data from many records into one record. This record gives information on the program name, program version, language, program running times, number of times used, last time used, username, and computer name. This summarization compresses the amount of data that is stored in the Configuration Manager database and is sent to the central site.

The summary data also includes the number of times each matching metered piece of software was run on a specific computer by a specific user during that month. This task is set to run every day by default, and the summary is done for a period of one month.



Real World Scenario

Manually Summarize Software Metering Data

As the Configuration Manager administrator, you have been requested to demonstrate the Software Metering feature. You need to ensure that all the latest data is summarized and is part of the reports. To do so, follow these steps:

1. Log on to the site server where you have the ConfigMgr 2012 Toolkit SP1 or higher version installed.
2. From (`%program files(x86)% )\Configmgr 2012 Toolkit SP1\ServerTools`, copy `runmetersumm.exe` to `<:>\Program Files\Microsoft Configuration Manager\bin\x64`.
3. Open a command prompt as administrator, and navigate to `<:>\Program Files\Microsoft Configuration Manager\bin\x64`.
4. Type **`runmetersumm.exe CM_<Configuration Manager site code>`**, for example, **`runmetersumm.exe CM_S01`**.
5. Press Enter, and notice the number of records that have been summarized.

Monitor Client Activity

Whenever a client runs a program, it will be registered in the `mtrmgr.log` file on the client. If the program has a matching software metering rule, the client agent will start tracking the process associated with the program, as shown in Figure 11.22.

Each client will generate a software metering usage report and send the report to the management point. You can initiate the action manually by running the Software Metering Usage Report Cycle action in the Configuration Manager Properties on the client, as shown in Figure 11.23.

Activity from this process is written to the `SWMTRReportGen.log` file on the client. The data will be sent to the site server and recorded in the `swmproc.log` file on the site server.

Default Software Metering Reports

Configuration Manager 2012 ships with several canned software metering reports:

- All Software Metering Rules Applied To This Site
- Computers That Have A Metered Program Installed But Have Not Run The Program Since A Specified Date
- Computers That Have Run A Specific Metered Software Program
- Concurrent Usage For All Metered Software Programs
- Concurrent Usage Trend Analysis Of A Specific Metered Software Program
- Install Base For All Metered Software Programs

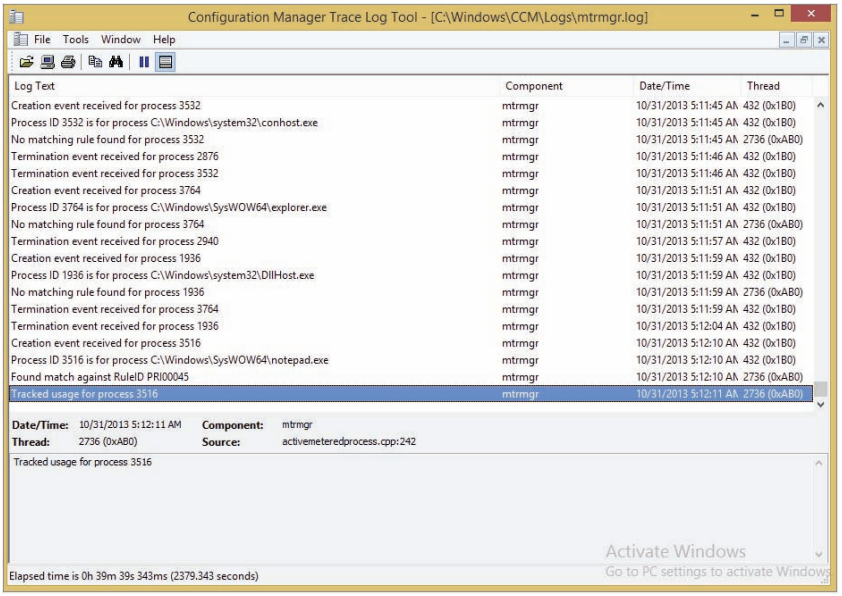


FIGURE 11.22
Reading the `mtrmgr.log` file on the client

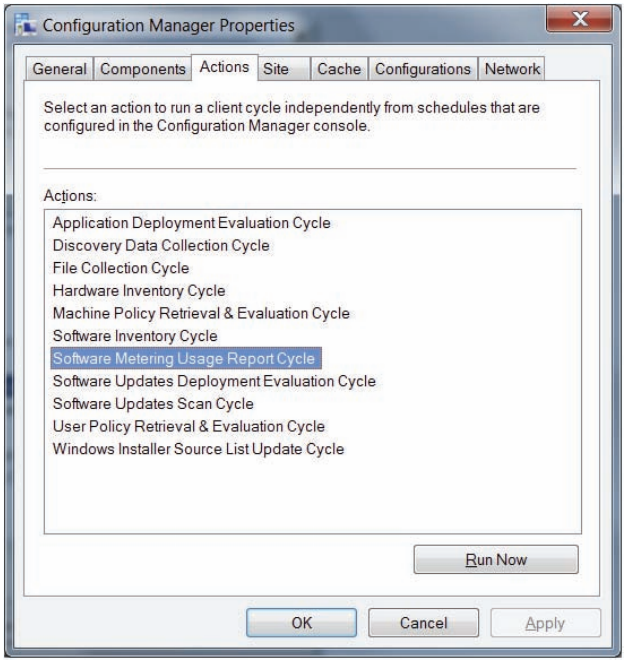


FIGURE 11.23
Running the Software Metering Usage Report Cycle action on the client

- Time Of Day Usage Summary For A Specific Metered Software Program
- Total Usage For All Metered Software Programs
- Total Usage For All Metered Software Programs On Windows Terminal Servers
- Total Usage Of Specific Metered Software Product
- Total Usage Trend Analysis For A Specific Metered Software Program
- Total Usage Trend Analysis For A Specific Metered Software Program On Windows Terminal Servers
- Users That Have Run A Specific Metered Software Program
- Software Metering Summarization Progress

One of the disadvantages of having a large number of disabled software metering rules is that all rules will be shown in the Install Base For All Metered Software Programs report. This might clutter the picture a little bit because you will see programs that you might not be interested in seeing.

By combining the values from the Install Base For All Metered Software Programs report with the Computers That Have A Metered Program Installed But Have Not Run The Program Since A Specified Date report, you can easily see how many installed instances you have and measure that against how many times the application has been used in a specific period. This will give the names of computers where you can uninstall the application and that way save money on the software budget.

The Bottom Line

Configure and manage Software Inventory. Configuring Software Inventory has changed in Configuration Manager 2012, although the client-processing part is almost the same as in Configuration Manager 2007.

> **Master It** By default, Configuration Manager does not inventory for any file types. Where would you go to do that?

Configure and manage Hardware Inventory. Hardware Inventory provides a wealth of information on the hardware resources in your organization. That information is vital when planning for things such as updating standard business software or upgrading the standard operating system your organization uses. If the standard hardware inventory collected is not enough for your needs, then you have many options to extend the hardware inventory to get that vital information.

> **Master It** Where do you enable or disable data classes in Hardware Inventory?

Configure and manage Software Metering. Keeping track of software that is installed and actually being used is a large part of being able to manage software licenses effectively. By pairing Software Metering in Configuration Manager with Software Inventory, you can get detailed information on just what software is out there and who is or is not using it. This goes a long way to help keep your software licensing in compliance.

> **Master It** How long do you have to wait, at the very least, after you configure Software Metering before you can expect to see any data returned?



Chapter 12

Asset Intelligence

System Center 2012 R2 Configuration Manager gives organizations better control over their information technology infrastructure and assets through Asset Intelligence technologies by enabling IT professionals to see what hardware and software assets they have, who is using them, and where they are. Asset Intelligence translates inventory data into information; this gives the IT professionals the ability to build reports to understand how these assets are being used in their environment.

ConfigMgr tracks nearly all the software assets on a network, providing comprehensive details about both physical and virtual applications installed across an enterprise. Asset Intelligence lets IT professionals define, track, and proactively manage conformity to configuration standards. Metering and reporting the deployment and the use of both physical and virtual applications help organizations make better business decisions about software licensing and maintenance of licensing agreements. In this chapter we will cover the aspects of Asset Intelligence in ConfigMgr 2012 and show you how to enable it to take full advantage of this information.

In this chapter, you will learn to

- Enable Asset Intelligence
- Configure the Asset Intelligence synchronization point
- Import the Microsoft Volume License Statement

Requirements for Asset Intelligence

The Asset Intelligence feature in ConfigMgr 2012 has both external and internal dependencies that you will need to consider when using this feature. Those requirements include the following:

- Client agent requirements
- Site maintenance task requirements
- Windows event log requirements

Client Agent Prerequisites

The Asset Intelligence reports are based on information gathered through hardware and software inventory. To get the necessary information from clients for all Asset Intelligence reports, you must enable these client agents:

- Hardware Inventory Client Agent
- Software Metering Client Agent

Hardware Inventory Client Agent Requirement

To be able to collect inventory data required for some Asset Intelligence reports, you must enable the Hardware Inventory Client Agent. In addition, some hardware inventory reporting classes that Asset Intelligence reports depend on must be enabled on primary site server computers. You saw how to do this in Chapter 11, "Inventory and Software Metering."

Reports That Require Software Metering

Six reports require the Software Metering Client Agent to be enabled before they can provide any data:

Software 07A Recently Used Executable Programs By The Count Of Computers

Software 07B Computers That Recently Used A Specified Executable Program

Software 07C Recently Used Executable Programs On A Specified Computer

Software 08A Recently Used Executable Programs By The Count Of Users

Software 08B Users That Recently Used A Specified Executable Program

Software 08C Recently Used Executable Programs By A Specified User

Maintenance Tasks

The following maintenance tasks are associated with Asset Intelligence. By default, both maintenance tasks are enabled and configured by default.

Check Application Title With Inventory Information This maintenance task checks to see if the software title that is reported in software inventory is reconciled with the software title in the Asset Intelligence Catalog. Basically it compares software hash from inventory to software code in the catalog to ensure accuracy and completeness. By default, this maintenance task is scheduled to run on Saturday after 12:00 a.m. and before 5:00 a.m.

Summarize Installed Software Data This maintenance task provides the information that is displayed in the Inventoried Software node under the Asset Intelligence node in the Assets and Compliance workspace. When the task runs, Configuration Manager gathers a count of all inventoried software titles at the primary site. This task is available only on primary sites. By default, this maintenance task is scheduled to run on Saturday after 12:00 a.m. and before 5:00 a.m.

To configure these maintenance tasks, do the following:

1. In the ConfigMgr console, click Administration.
2. In the Administration workspace, expand Site Configuration, and then click Sites.
3. Select the site on which to configure the Asset Intelligence maintenance task.

4. On the Home tab of the ribbon, in the Settings group, click Site Maintenance.

   A list of all available maintenance tasks will appear, as shown in Figure 12.1.

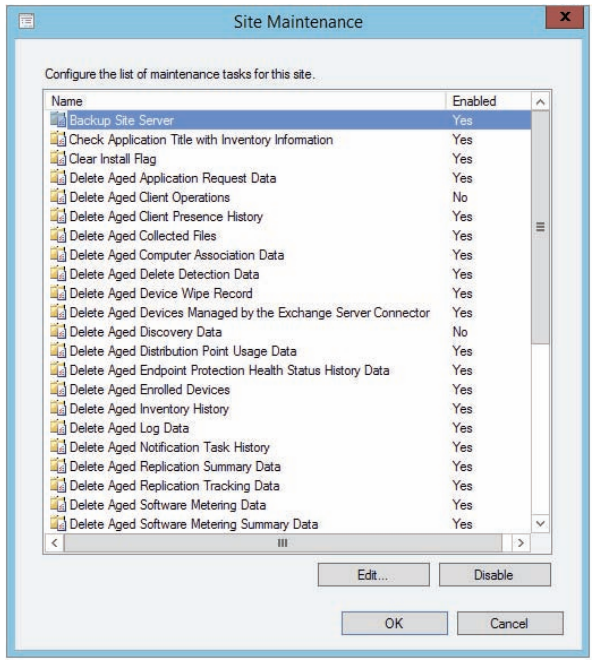


FIGURE 12.1 Site Maintenance dialog

5. Choose the desired maintenance task, and then click Edit to modify the settings.
6. Enable and configure the maintenance task.
7. Click Apply to save your settings.

The task will now run according to its schedule. If you want to know more about this maintenance task, check Chapter 19, "Troubleshooting."

Windows Ekvent Log Settings

Four Asset Intelligence reports display data gathered from the Windows security event logs on client computers. If the security event log is not set up properly, these reports will be empty even if the appropriate hardware inventory class has been enabled. We will discuss configuring these settings later in the chapter. The following reports require these collected events:

Hardware 3A Primary Computer Users

Hardware 3B Computers For A Specific Primary Console User

Hardware 4A Computers With Multiple Users (Shared)

Hardware 5A Console Users On A Specific Computer

To enable auditing of success logon events, follow these steps:

1. On a domain controller computer, navigate to Administrative Tools ➢ Group Policy Management.
2. Navigate to Default Domain Policy, right-click Default Domain Policy and choose Edit ➢ Computer Configuration ➢ Policies ➢ Windows Settings ➢ Security Settings ➢ Local Policies ➢ Audit Policy.
3. In the results pane, double-click Audit Logon Events, and ensure that Success is selected.

Elements of Asset Intelligence

Asset Intelligence enhances the inventory capabilities of ConfigMgr 2012 by extending hardware and software inventory. The Asset Intelligence category now contains more than 60 reports that present this information in an easy-to-use format. Most reports link to more detailed reports that allow the administrator to query for general information and drill down to more detailed information as needed.

Asset Intelligence Catalog

The ConfigMgr 2012 Asset Intelligence Catalog is a set of tables stored in the ConfigMgr database containing categorization and identification data for more than 300,000 software titles and versions that are divided into almost 100 families and almost 2,000 specific categories. These database tables are also used to manage hardware requirements for specific software titles.

With ConfigMgr 2012, the Asset Intelligence Catalog was enhanced to allow software titles in use (both Microsoft and general software) to be manually imported. In addition, it now includes a large collection of known hardware requirements for software titles stored in the Asset Intelligence Catalog. Also, it is now possible to edit the local Asset Intelligence Catalog and to upload software title information to System Center Online (SCO) for categorization.

What Is System Center Online?

Hosted by Microsoft, System Center Online is "software as a service," an online management service aimed at the IT community. Some of the services that will be eventually hosted are antivirus, anti-spyware, system monitoring, backup/restore, policy management, and, in the case of ConfigMgr, asset inventory monitoring.

Asset Intelligence Catalog updates containing newly released software and hardware definitions will be available for download periodically for bulk catalog updates, or the catalog can be dynamically updated by Microsoft Software Assurance (SA) customers using the Asset Intelligence synchronization point site system role.

Software Categories

Administrators can view available software category information stored in the Asset Intelligence Catalog by using the Assets and Compliance ➢ Overview ➢ Asset Intelligence ➢ Catalog view in the ConfigMgr console.

These software categories are used to give broad listings of inventoried software titles and are also used as high-level groupings of more detailed software families. The Asset Intelligence Catalog has many predefined software categories, and you can create user-defined categories to continue to define inventoried software as needed. For example, the predefined E-mail And Collaboration category includes applications such as Microsoft Outlook and Outlook Express. The validation state for software categories already defined is always validated, while custom category information added to the Asset Intelligence catalog is user-defined. Note that predefined software category information is read-only and can't be changed. User-defined software categories can be added, modified, or deleted by administrators. We will cover managing software categories later in the chapter in the section "Asset Intelligence Validation States."

Software Families

Administrators can view available software family information stored in the Asset Intelligence Catalog by using the Assets and Compliance ➢ Overview ➢ Asset Intelligence ➢ Catalog view in the ConfigMgr console.

Software families in Asset Intelligence are used to define inventoried software even further within software categories. For example, the Security software family is defined by the Security and Security Threat labels. Like software categories, predefined software families always have a validation state of validated, while custom software family information has a state of user-defined. Also like software categories, predefined software family information can't be modified.

Software Labels

You can create custom software labels to even further categorize inventoried software titles that are in the Asset Intelligence Catalog. Administrators can use custom labels to create user-defined groups of software titles that share a common attribute. For example, a custom label could be called *bank software*, and that label would be used to identify inventoried bank software titles, which in turn could be used in a report to show all software that has that label. Custom labels have no validation state since they are always created locally in your ConfigMgr hierarchy.

In the ConfigMgr console, you can view all the custom labels that you or another administrator has made in the Asset Intelligence Catalog by choosing Asset Intelligence ➢ Catalog.

Inventoried Software

The Inventoried Software node is located under Asset Intelligence ➢ Inventoried Software in the ConfigMgr console. Administrators can look at inventoried software title information collected from ConfigMgr clients in this node and can even create up to three custom labels per inventoried software item to further utilize user-defined categorization.

Each software title shows the following information:

- Name of the software title
- Name of the software vendor

- Product version
- Assigned software category
- Assigned software family

All of this information except for version can be changed, via a local edit. Anything that can be changed can be reverted to the original values later.

Hardware Requirements

With the Asset Intelligence ➢ Hardware Requirements node, you can manage software title hardware requirements data that is stored in the Asset Intelligence Catalog. The hardware requirements that are preloaded into the Asset Intelligence Catalog are not based on inventoried software information but are included as part of the Asset Intelligence Catalog. In addition to the default hardware requirements listed in this node, administrators can add new software title hardware requirements as needed to meet custom report requirements. The information that is displayed in this node includes the following:

- Name of the software title that the hardware requirement is for
- Validation state for the hardware requirement (System Center Online requirements are always validated; custom hardware requirements are always user-defined.)
- Minimum processor speed, in MHz, that the software title requires
- Minimum RAM, in KB, that the software title requires
- Minimum free disk space, in KB, that the software title requires
- Minimum hard disk size, in KB, that the software title requires

As in other parts of the Asset Intelligence Catalog, custom hardware requirements for software titles that aren't stored in the catalog can be modified, but the predefined information is read-only and can't be changed or deleted.

Asset Intelligence Validation States

Asset Intelligence validation states show the source and current validation status of Asset Intelligence Catalog information. They are outlined in Table 12.1, which is reproduced from the ConfigMgr documentation.

Table 12.1: Asset Intelligence validation states

State	Definition	Administrator Action	Comment
Validated	Catalog item has been defined by System Center Online (SCO) researchers.	None	This is the best state.
User-defined	Catalog item has not been defined by SCO researchers.	Customized the local catalog information	This state will be shown in Asset Intelligence reports.

State	Definition	Administrator Action	Comment
Pending	Catalog item has not been defined by SCO researchers but has been submitted for categorization.	Requested categorization from SCO	The catalog item will remain in this state until SCO categorizes the item and the Asset Intelligence Catalog is synchronized.
Updateable	A user-defined catalog item has been categorized differently by SCO.	Customized the local Asset Intelligence Catalog to categorize an item as user-defined	The administrator can use the Software Details Conflict Resolution dialog box to choose which category to use.
Uncategorized	Catalog item has not been defined by SCO; the item has not been submitted to SCO and has not been categorized by admin.	None	Request categorization or customize local catalog. This is the base state of all unknown software.

Asset Intelligence Synchronization Point

ConfigMgr has a site system role for Asset Intelligence called the Asset Intelligence synchronization point. This site system role is used to connect to System Center Online over TCP port 443 so dynamic Asset Intelligence Catalog updates can be managed.

This site role can be installed only on the ConfigMgr 2012 Central Administration Site (CAS)/stand-alone primary site, and all of your Asset Intelligence Catalog customization must be done on a ConfigMgr console that is connected to this site. You must configure all the updates at the central site, but all Asset Intelligence Catalog information is replicated to all child primary sites using ConfigMgr SQL replication. If a CAS doesn't exist in the environment, you can configure this on the stand-alone primary site server.

Using the Asset Intelligence synchronization point, Software Assurance (SA) license customers can also request on-demand catalog synchronization with System Center Online or schedule automatic catalog synchronization, and they can upload uncategorized software titles to System Center Online for identification.

The Asset Intelligence Home Page

With ConfigMgr 2012, an Asset Intelligence home page was added to the ConfigMgr console; it's similar to home pages in some of the other features, such as Software Updates.

To display the Asset Intelligence home page, do the following in the ConfigMgr console: Select Assets and Compliance ➢ Overview ➢ Asset Intelligence. Figure 12.2 shows an example of the Asset Intelligence home page.

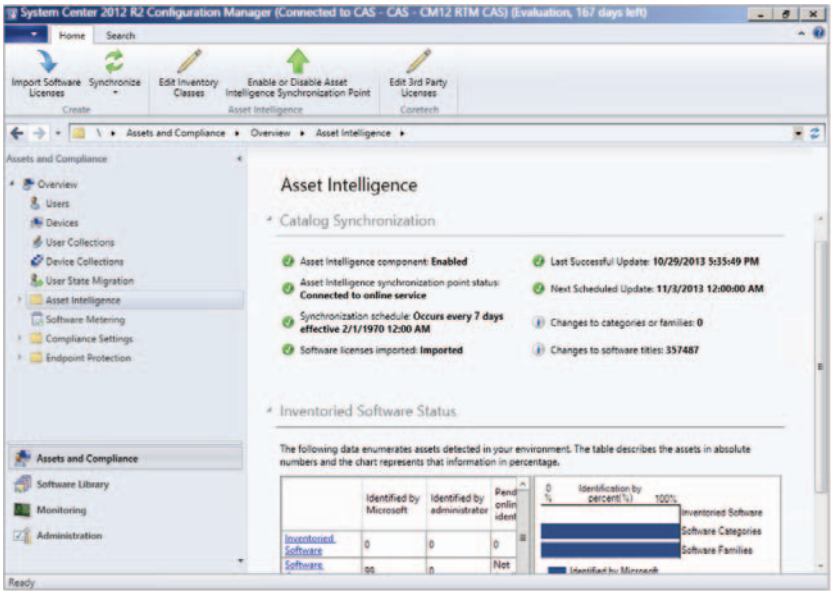


FIGURE 12.2
Asset Intelligence home page

The Asset Intelligence home page is divided into the following sections:

- Catalog Synchronization
- Inventoried Software Status

Asset Intelligence Catalog Synchronization

This section displays the following information:

Asset Intelligence Component This item displays the status of the component as either Enabled or Disabled.

Asset Intelligence Synchronization Point Status This item displays the online status of the synchronization point or any failure that happened during this synchronization.

Synchronization Schedule This item matches the configured schedule of the catalog; by default, this is set for every 7 days, but you can change this on the Assets and Compliance ➢ Asset Intelligence node. Right-click the node, choose Synchronize ➢ Schedule Synchronization, and choose the desired schedule.

Software Licenses Imported This item shows whether the Microsoft volume license has been imported into the ConfigMgr database.

Last Successful Update This item shows the last time Configuration Manager was able to synchronize the catalog. If it was not able to synchronize, a warning icon will show and will display a Not Applicable status.

Next Scheduled Update This item displays the next date and time when the catalog will synchronize.

Changes To Categories Or Families This item displays the number of changes or updates in categories that occurred on the database during the last synchronization with System Center Online.

Changes To Software Titles This item displays the number of changes or updates in software titles that occurred during the last synchronization with System Center Online.

Inventoried Software Status

The following data enumerates assets detected in the ConfigMgr environment. The table describes the assets in absolute numbers, and the chart represents that information in percentages.

Inventoried Software Status Table This item displays the assets of the Asset Intelligence Catalog in summary table format with the following information:

- Inventoried Software
- Software Categories
- Software Families

Each of these is shown in one of the following states:

- Identified By Microsoft
- Identified By Administrator
- Pending Online Identification
- Unidentified And Not Pending

Identification By Percent Chart This item displays an Asset Catalog summary in bar chart format, including the following information as percentages:

- Inventoried Software
- Software Categories
- Software Families

These in turn are shown color coded for easier identification:

- Identified By Microsoft
- Identified By Administrator
- Pending Online Identification
- Unidentified And Not Pending

Asset Intelligence Reports

To see the real power behind the Asset Intelligence feature, you have to examine the various Asset Intelligence reports that are provided with ConfigMgr right out of the box.

You can find the Asset Intelligence reports in the ConfigMgr console by choosing Monitoring ➢ Overview ➢ Reporting. Expand Reports and click Asset Intelligence. The numbers in the installed software and license information shown in Asset Intelligence reports may vary from the true number of software products installed or licenses in use on your network because of complex dependencies and limitations in inventorying software license information for software titles installed in an enterprise environment. Therefore, you should not use Asset Intelligence reports as the sole source of deciding how many software licenses to purchase for compliance.

The following are example dependencies that are involved in inventorying installed software and licenses in an enterprise using Asset Intelligence that might affect the accuracy of the data:

Client Hardware Inventory Dependency Asset Intelligence–installed software reports are based on data collected from ConfigMgr clients by extending hardware inventory to enable Asset Intelligence reporting. Because of this, Asset Intelligence reports will report data only from ConfigMgr clients that have completed a hardware inventory scan successfully and have the required Asset Intelligence WMI reporting class enabled. Also, since hardware inventory runs on a schedule that is set by the administrator, there may be a delay in data being reported that might affect the accuracy of Asset Intelligence reports at any given time.

Software Packaging Dependencies Because Asset Intelligence reports are based on installed software title data using standard ConfigMgr client hardware inventory processes, some of that data might not be collected properly if the software executables don't conform to standard installation processes or have been modified prior to installation.

Server Role Dependencies When you're using CAL reporting, it is important to remember that these reports were designed to provide visibility into the specific usage of products in specific scenarios, such as a Windows server hosting only one server role. In cases where a Windows server is hosting more than one role, this might cause inaccurate Asset Intelligence reports.

Location And Usage Remember that Asset Intelligence reports were designed to report license usage, not how many licenses have been actually bought and for what purpose they are allowed to be used.

Hardware Reports

Asset Intelligence hardware reports provide information about hardware assets in your organization, such as a computer's age and its ability to handle a software upgrade. Some reports are based on information collected from the System Security event log, so you should clear that log if a computer is assigned to another user. The following hardware Asset Intelligence reports are available:

Hardware 01A Summary Of Computers In A Specific Collection

Hardware 03A Primary Computer Users

Hardware 03B Computers For A Specific Primary Console User

Hardware 04A Computers With Multiple Users (Shared)

Hardware 05A Console Users On A Specific Computer

Hardware 06A Computers For Which Console Users Could Not Be Determined

Hardware 07A USB Devices By Manufacturer

Hardware 07B USB Devices By Manufacturer And Description

Hardware 07C Computers With A Specific USB Device

Hardware 07D USB Devices On A Specific Computer

Hardware 08A Hardware That Is Not Ready For A Software Upgrade

Hardware 09A Search For Computers

Hardware 10A Computers In A Specified Collection That Have Changed Within A Specified Timeframe

Hardware 10B Changes On A Specified Computer Within A Specified Timeframe



Real World Scenario

Planning for a Software Upgrade

You get word from your manager that the department responsible for all the company training manuals is working on updating many of the manuals because of some new federal regulations. They are making these updates with a new version of the Adobe Acrobat software, and there is a possibility that you might have to deploy Acrobat Reader X so that employees will be able to read the updated manuals properly.

The company is also in the middle of a hardware refresh, so your manager is concerned that there may be computers on the network that do not have the necessary hardware requirements to run Acrobat Reader X properly, so she wants to use ConfigMgr to generate a list of those computers if there are any.

Hearing this, you are glad that you have already enabled Asset Intelligence, because there is a specific report for just this scenario. To meet your manager's request, just go to the report Hardware 08A: Hardware That Is Not Ready for a Software Upgrade. Since you are concerned with user computers in this instance, select the desired collection in the Collection field. The Asset Intelligence knowledge base, which is part of the ConfigMgr database, already has information about Acrobat Reader X, so select that for the Product field.

After you run the report, you can provide that link to your manager so she can either print it or export it into Excel for her own use.

Software Reports

Software Asset Intelligence reports provide information about software families, categories, and specific software titles installed on computers within your organization. The following software Asset Intelligence reports are available:

Software 01A Summary Of Installed Software In A Specific Collection

Software 02A Product Families For A Specific Collection

Software 02B Product Categories For A Specific Product Family

Software 02C Software In A Specific Product Family And Category

Software 02D Computers With Specific Software Installed

Software 02E Installed Software On A Specific Computer

Software 03A Uncategorized Software

Software 04A Software Configured To Automatically Run On Computers

Software 04B Computers With Specific Software Configured To Automatically Run

Software 04C Software Configured To Automatically Run On A Specific Computer

Software 05A Browser Helper Objects

Software 05B Computers With A Specific Browser Helper Object

Software 05C Browser Helper Objects On A Specific Computer

Software 06A Search For Installed Software

Software 07A Recently Used Executable Programs By The Count Of Computers

Software 07B Computers That Recently Used A Specified Executable Program

Software 07C Recently Used Executable Programs On A Specified Computer

Software 08A Recently Used Executable Programs By The Count Of Users

Software 08B Users That Recently Used A Specified Executable Program

Software 08C Recently Used Executable Programs By A Specified User

Software 09A Infrequently Used Software

Software 09B Computers With Infrequently Used Software Installed

Software 10A Software Titles With Specific, Multiple Custom Labels Defined

Software 10B Computers With A Specific Custom-Labeled Software Title Installed

Software 11A Software Titles With A Specific Custom Label Defined

Software 12A Software Titles Without A Custom Label

License Management Reports

The following license management Asset Intelligence reports are available:

License 01A Microsoft Volume License Ledger For Microsoft License Statements

License 01B Microsoft Volume License Ledger Item By Sales Channel

License 01C Computers With A Specific Microsoft Volume License Ledger Item And Sales Channel

License 01D Microsoft Volume License Ledger Products On A Specific Computer

License 02A Count Of Licenses Nearing Expiration By Time Ranges

License 02B Computers With Licenses Nearing Expiration

License 02C License Information On A Specific Computer

License 03A Count Of Licenses By License Status

License 03B Computers With A Specific License Status

License 04A Count Of Products Managed By Software Licensing

License 04B Computers With A Specific Product Managed By Software Licensing Service

License 05A Computers Providing Key Management Service

License 06A Processor Counts For Per-Processor Licensed Products

License 14A Microsoft Volume Licensing Reconciliation Report

License 14B List Of Microsoft Software Inventory Not Found In Mvls

License 15A General License Reconciliation Report

License 15B General License Reconciliation Report By Computer

Configuring Asset Intelligence

ConfigMgr Asset Intelligence is enabled by default. Depending on what data you want information on, you will have to do the following:

1. Choose the Assets And Compliance workspace in the ConfigMgr console.
2. Under Overview, right-click Asset Intelligence, and click Edit Inventory Classes.
3. Choose to enable only the desired Asset Intelligence reporting class.
4. Make sure that certain client agents are enabled, which we will go over in the following sections.

Enabling Asset Intelligence

To successfully collect data for the hardware and software reports in Asset Intelligence, you first need to enable the Hardware Inventory Client Agent.

The classes that are used for the hardware and software inventory reports include the following:

```
SMS_SystemConsoleUsage

SMS_SystemConsoleUser

SMS_InstalledSoftware

SMS_AutoStartSoftware

SMS_BrowserHelperObject

SoftwareLicensingService

SoftwareLicensingProduct

Win32_USBDevice

SMS_SoftwareTag
```

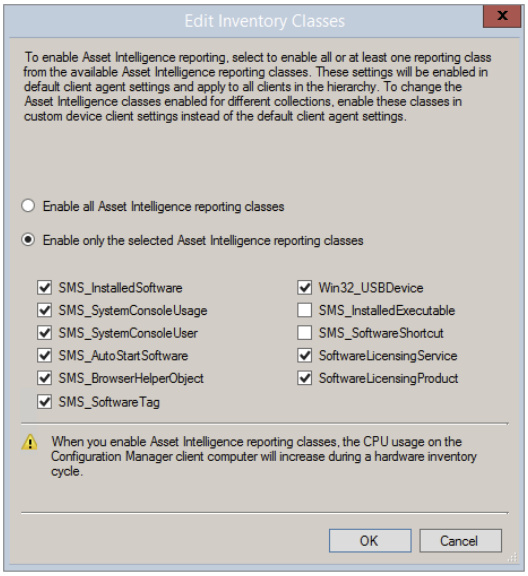


FIGURE 12.3
Asset Intelligence Edit Inventory Classes dialog box

To enable one or all of these classes in ConfigMgr, you have to follow these steps:

1. Choose Assets and Compliance ➢ Overview ➢ Asset Intelligence.
2. Right-click, and choose Edit Inventory Classes. Figure 12.3 shows the dialog box that opens.
3. Choose the inventory classes that need to be enabled, and click OK.

After you do that, it could take up to a few days for these changes to take full effect, depending on your ConfigMgr hierarchy and how often you have the Hardware Inventory Client Agent set to collect inventory.

Installing an Asset Intelligence Synchronization Point

As discussed earlier in the chapter, the Asset Intelligence synchronization point role is used to connect ConfigMgr sites to System Center Online to synchronize Asset Intelligence catalog information. You can install this role only on a site system located in the CAS of a ConfigMgr hierarchy, and you'll require Internet access to synchronize with System Center Online on TCP port 443. The Asset Intelligence synchronization point can also upload custom software title information to System Center Online for categorization. All information uploaded to System Center Online will be treated as public information by Microsoft, so you should be sure that your custom information does not contain any sensitive information.

To install the Asset Intelligence synchronization point and have it be secure, you can acquire an optional System Center Online authentication certificate (`*.pfx`), which can be acquired only by SA license customers. (For more information on Software Assurance, check out the SA

website at `www.microsoft.com/licensing/sa/default.mspx`.) Before you begin the installation of the Asset Intelligence synchronization point, make sure that all of the following are true:

- You have a valid SCO authentication certificate. If you don't have one, do not put any certificate information in the field since this certificate is optional.
- The Asset Intelligence synchronization point will be available on a shared network folder accessible to the server where you will be running the New Site Role Wizard.
- The Asset Intelligence synchronization point will stay in that location until the Asset Intelligence synchronization point has done its first synchronization with System Center Online.

To install an Asset Intelligence synchronization point, follow these steps:

1. In the ConfigMgr console, select Administration ➢ Overview ➢ Site Configuration ➢ Sites.
2. Select CAS Site Server Name. Choose the Home tab of the ribbon, and click Add Site System Roles to start the Add Site System Roles Wizard.
3. As you have done with other ConfigMgr wizards covered in this book, verify the site system settings on the General page, and click Next.
4. On the Proxy page, enter information as needed, and click Next.

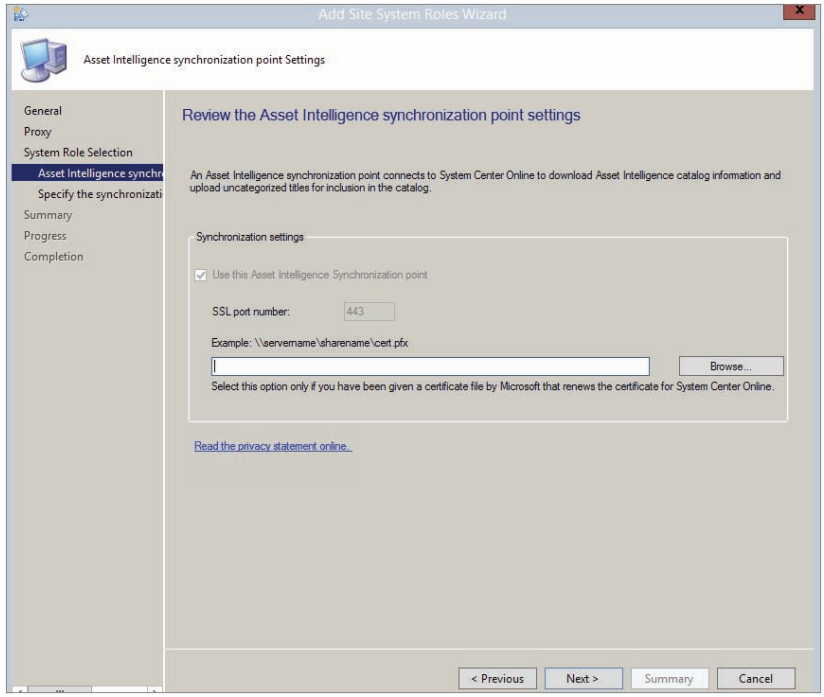


FIGURE 12.4 Asset Intelligence Synchronization Point Settings page

5. On the System Role Selection page, select the Asset Intelligence Synchronization Point check box, and then click Next.
6. On the Asset Intelligence Synchronization Point Settings page, you can set up an optional certificate. If you choose to do so, then set the path to the SCO authentication certificate (`*.pfx`) file, as shown in Figure 12.4, and click Next.
7. On the Proxy Server Settings page, configure the settings for the proxy server if needed.
8. On the Synchronization Point Schedule page, you can choose whether to set up synchronization on a simple or custom schedule, as you've seen in other ConfigMgr options.
9. On the Summary page of the wizard, review the settings you have specified to make sure they are correct. If you need to make any changes, click the Previous button. Otherwise, click Next to finish the rest of the configuration.

Import Software License into Asset Intelligence

One of the most important pieces of Asset Intelligence is the availability to import the current Microsoft Volume License Summary into the database for better reporting of this license count. Also, you can import a non-Microsoft product license count into the database by selecting the option to upload a General License Statement file.

As shown in Figure 12.5, you can now import the Microsoft Volume License Statement or General License Statement in one easy wizard. First, select the type of file you are going to import. This will be either an `.xml` or `.csv` file for the Microsoft Volume License Statement or

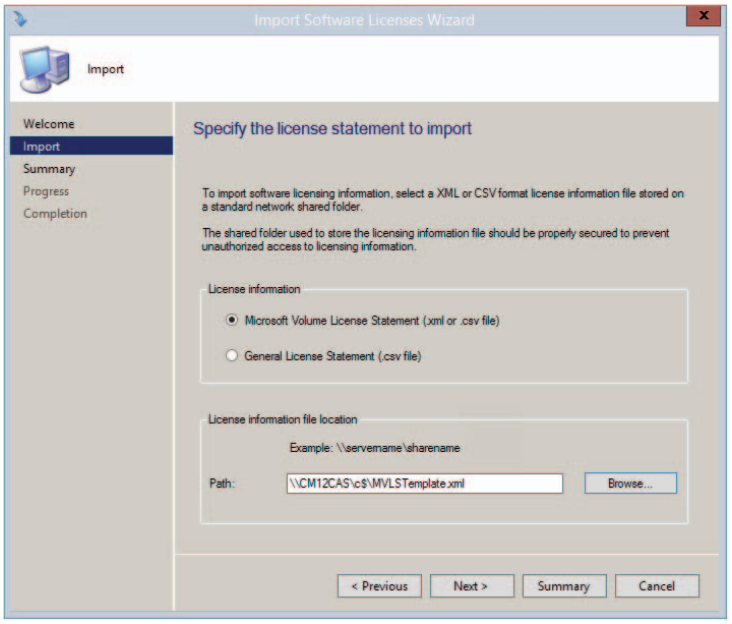


FIGURE 12.5 Import Software Licenses Wizard

a `.csv` file for the General License Statement. Once you have chosen the file you are going to upload, this information will be imported into the ConfigMgr database. On the next hardware and software inventory, the data will be analyzed, and the new imported license count will be available for the IT administrator's analysis. You can upload the license information as many times as needed to update the license or when the enterprise agreement of the Microsoft product gets updated. You'll need to follow the same process for the non-Microsoft product when you want to review the license count.

Importing Software License Information

The following sections describe the procedures necessary to import both Microsoft and general software licensing information into the ConfigMgr 2012 site database using the Import Software Licenses Wizard. When you import software licenses from license information files into the site database, the site server computer account requires Full Control NTFS permissions to the file share that will be used to import software license information. When this license information gets imported into the site, the existing software license information file used with the Import Software Licenses Wizard contains a complete list of all necessary software license information.

Follow these steps to import the software license:

1. In the Assets And Compliance workspace, click Asset Intelligence.
2. On the Home tab of the ribbon, in Create Group, click Import Software Licenses.

   The Import Software Licenses Wizard opens, as shown in Figure 12.5.
3. On the Welcome page, click Next.
4. On the Import page, specify whether you are importing a Microsoft Volume License Statement (`.xml` or `.csv`) or a General License Statement (`.csv`).
5. Enter the UNC path to the license information file, or click Browse to select a network shared folder and file.
6. On the Summary page, review the information you have specified to ensure that it is correct before continuing.

   If you need to make changes, click Previous to return to the Import page. Otherwise, click Next.
7. Once this is completed, click Close.

Perform the following steps for the General License Statement as well; just make sure to select this in step 4.

Creating the Microsoft Volume License Statement

Before you start the process of creating the Microsoft Volume License Statement, make sure you have access to `http://licensing.microsoft.com/`. If you don't have access, please talk to your Microsoft Account Manager or Microsoft Technical Account Manager and ask them to send you your License Summary. Once you have the proper access, select the License Summary from the licensing site, and export it to Excel. When you have it in Excel, make sure the following fields and values are selected, with example data shown here.

Product Pool	License Product Family	License Version	Effective Quantity	Unresolved Quantity
Applications	Access	2010	70	0

Once you have imported the Microsoft Volume License Statement, you can run any of the reports with the title "License."

Creating the General License Statement

Now let's look at an example of the General License Statement. To create this you need to manually create a `.csv` file with the fields you need and list the software for which you want ConfigMgr to keep track of the license count. Once you finish creating the file, follow the same steps as you did to import the software license, but now use the example shown in Figure 12.6.

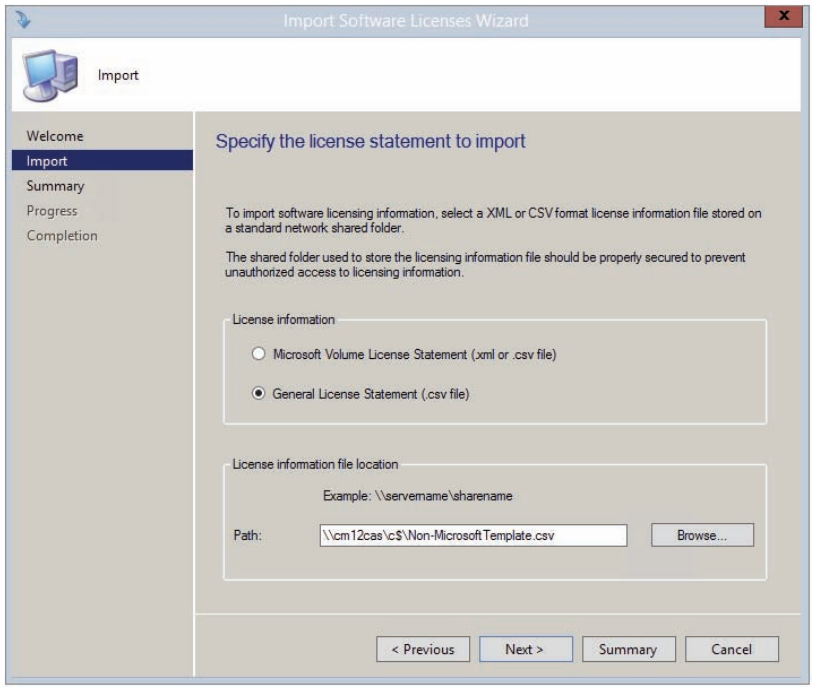
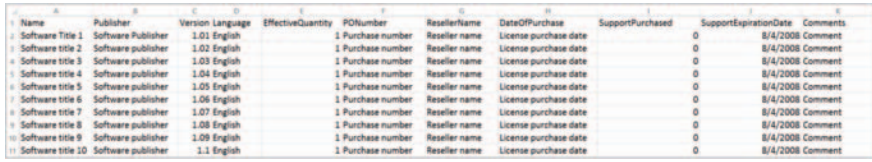


FIGURE 12.6 General License Statement import



Name	Publisher	Version	Language	EffectiveQuantity	PONumber	ResellerName	DateOfPurchase	SupportPurchased	SupportExpirationDate	Comments
Software Title 1	Software Publisher	1.01	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 2	Software publisher	1.02	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 3	Software publisher	1.03	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 4	Software publisher	1.04	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 5	Software publisher	1.05	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 6	Software publisher	1.06	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 7	Software publisher	1.07	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 8	Software publisher	1.08	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 9	Software publisher	1.09	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment
Software title 10	Software publisher	1.1	English		1 Purchase number	Reseller name	License purchase date	0	8/4/2008	Comment

FIGURE 12.7 General License Statement

As you can see in Figure 12.7, all you need to do is create the `.csv` file and list the third-party software for which it needs to keep track of the license count.

The following is a list of reports that you can run:

License 14A Microsoft Volume Licensing Reconciliation Report

License 14B List Of Microsoft Software Inventory Not Found In MVLS

License 15A General License Reconciliation Report

License 15B General License Reconciliation Report By Computer

The Bottom Line

Enable Asset Intelligence. If you installed ConfigMgr from scratch, you will find that Asset Intelligence is not enabled by default. Depending on the data that you want information on, you will have to select the ConfigMgr Asset Intelligence reporting classes and make sure that client agents are enabled.

Master It Which classes in the Asset Intelligence Edit Inventory Classes dialog do you have to enable to use Asset Intelligence?

Configure the Asset Intelligence synchronization point. The Asset Intelligence synchronization point is used to connect to System Center Online to synchronize Asset Intelligence Catalog information and get periodic updates.

Master It What do you need to do in order to configure the Asset Intelligence synchronization point?

Import the Microsoft Volume License Statement. In ConfigMgr you can import the Microsoft Volume License Statement and the General License Statement so that the software inventory and Asset Intelligence can count the number of licenses currently in use in the environment.

Master It What file types does ConfigMgr 2012 support for the license statements?



Chapter 13

Reporting

Configuration Manager reports are now fully enabled for role-based administration. The data for all reports included with Configuration Manager is filtered based on the permissions of the administrative user who runs the report. As such, reporting in Configuration Manager has grown from being a feature mainly used to view inventory information to become one of the primary features. Reporting helps you to gather, organize, and present information such as the following:

- Administrative security
- Inventory information
- Software update compliance data
- Migration information
- Audit information
- Power management information
- Alert information
- User data
- Mobile device
- Client health
- Compliance and settings
- Replication traffic
- Operating system deployment
- Virtual applications
- Endpoint protection

In Configuration Manager 2012, the Reporting feature has changed from earlier releases of the product. Gone are the ASP web reports, and the only supported reporting solution left is SQL Server Reporting Services (SSRS). Using SQL Server Reporting Services gives you as an administrator several benefits compared to the classic web reports, such as these:

- Fully enabled for role-based administration
- Schedule reports to render during non-business hours
- Execute reports from a cache
- Create snapshots
- Subscribe to reports and have them mailed to you based on a schedule
- More easily modify existing reports with custom logos, text, and chart objects
- No 10,000-row limitations
- Standard reporting engine used by other Microsoft applications like SharePoint and the other Microsoft System Center applications

Another great feature of using reports is that you can allow users outside the IT department to view part of the rich information that is being gathered through Configuration Manager 2012. Viewing reports does not require access to the Configuration Manager administrative console, only membership in the appropriate groups. With that in mind, in this chapter you will learn skills that will help you install and manage Reporting Services as well as modify and create reports.

In this chapter, you will learn to

- Install the Reporting Services point
- Manage reporting security
- Create and manage report subscriptions
- Create custom reports

Installing SQL Server Reporting Services

Prior to installing the SQL Server reporting services role you need to ensure that you have installed SQL Server Reporting Services. SSRS can be found on the SQL DVD media you used to install SQL Server.

Before you install SSRS, you need to make sure that the server meets the minimum requirements:

- SQL Server 2008 with Service Pack 1 (SP1) Reporting Services
- .NET Framework 4

For a list of recommended hardware and software requirements for SQL Server 2008, see `http://technet.microsoft.com/en-us/library/ms143506(SQL.100).aspx#SEx64`.

Considerations for Installing SQL Server Reporting Services

There are several considerations prior to installing SQL Server Reporting Services, such as which extra tools to install, security, where to place the site system role, and SQL instance support. This section will try to answer what are considered to be the most common considerations.

With the installation of SSRS you not only install a reporting engine, but you also install the following:

- The report server web service
- Report Builder
- Reporting Services configuration tool
- Command-line utilities, such as `rsconfig.exe`, `rs.exe`, and `rskeymgmt.exe`

Besides the core tools and services, you should consider installing these features:

Business Intelligence Development Studio When you select to install Business Intelligence Development Studio (BIDS) using the SQL media, it will install Visual Studio and provide you reporting and report model design tools. This tool comes in very handy for creating more advanced reports and report models.

SQL Server Management Studio The client tools feature on the SQL media gives you SQL Server Management Studio, which is another tool often used in the report-creation process. SQL Server Management Studio is also used to configure SQL maintenance jobs, configure SQL security, and provide a GUI for maintaining the databases.

You also choose modes and instances:

Installation Mode During setup you can choose between Native mode or SharePoint mode. Configuration Manager 2012 supports only Native mode.

Instance You can install SQL Server Reporting Services in either the default instance or a named instance. Additionally, the instance you use can be shared with other System Center products as long as the other System Center products do not have restrictions for sharing the instance of SQL Server.

Where to Install the Reporting Services

The reporting site system can be installed on any primary site or the Central Administration Site. It is considered best practice to install the site system on the Central Administration Site. At the Central Administration Site you will have access to all global data and all site data. Installing the site system on a primary site will allow you to display only global data and site data that are local to the corresponding site. Installing the site system on a secondary site is not supported.

You can install the site system on the site server or on a remote server. For performance reasons it is often best to have a specific server acting as a reporting server. However, this all depends on several factors such as hardware and number of resources. Some IT professionals claim that splitting SQL services from the Central Administration Site leaves a server with very little work to do.

Security

Unlike SQL Server Reporting Services integration in Configuration Manager 2007 R2, Configuration Manager 2012 will connect to SQL and set the necessary permissions in Reporting Services. This eliminates the need to go into Reporting Services Configuration Manager and manually configure security. The security settings will be Credentials Stored Securely In The Report Server and Use As Windows Credentials When Connecting To The Data Source.

Installation of the Reporting Services Site System

The reporting site system role is one of the first roles you should install. Prior to installing the site system, you should verify that SQL Server Reporting Services is installed correctly and works as expected.

For installation and configuration information, read this TechNet article: `http://technet.microsoft.com/en-us/library/gg712698.aspx`.

For detailed information about SQL Server Reporting Services, read this TechNet article: `http://technet.microsoft.com/en-us/library/ms159106.aspx`.

The account that you use to install the site system role must have Read access to the database. To retrieve information about named instances, the user must also have Read access to WMI on the site system. To install a SQL Server Reporting Services point, take the following steps:

1. In the Configuration Manager administrative console, select the Administration workspace and navigate to Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Select the server where you want to install the role:
   - From the ribbon click Add Site System Roles to start the Add Site System Roles Wizard.
   - If you want to install the role on a new server, click Create Site System Server.
3. On the General page, click Next.
4. On the Proxy page, enter the appropriate information, and then click Next.
5. On the System Role Selection page, select Reporting Services Point from the list of available roles, and click Next.
6. On the Reporting Services Point Settings page, you must create the data source.

   A data source (or database connection) includes the data source type, connection information, and authentication settings used when connecting. The wizard will automatically create the data source based on the information you configure on this page in the wizard.
7. The wizard will discover the name of the site database server and the Configuration Manager database. To specify a named instance, type ***<Server Name>\<Instance Name>***.
8. To verify the settings in the Site Database and Database Name fields, click the Verify button.
9. The folder name will default to `ConfigMgr_<Sitecode>`; you can change the folder name if you want.

10. In the Authentication Settings area, click Set and choose an existing Configuration Manager account or select a new account.

    It is considered best practice to have a specific low-rights user account for Authentication settings.

11. Once all settings are configured as shown in Figure 13.1, click Next.

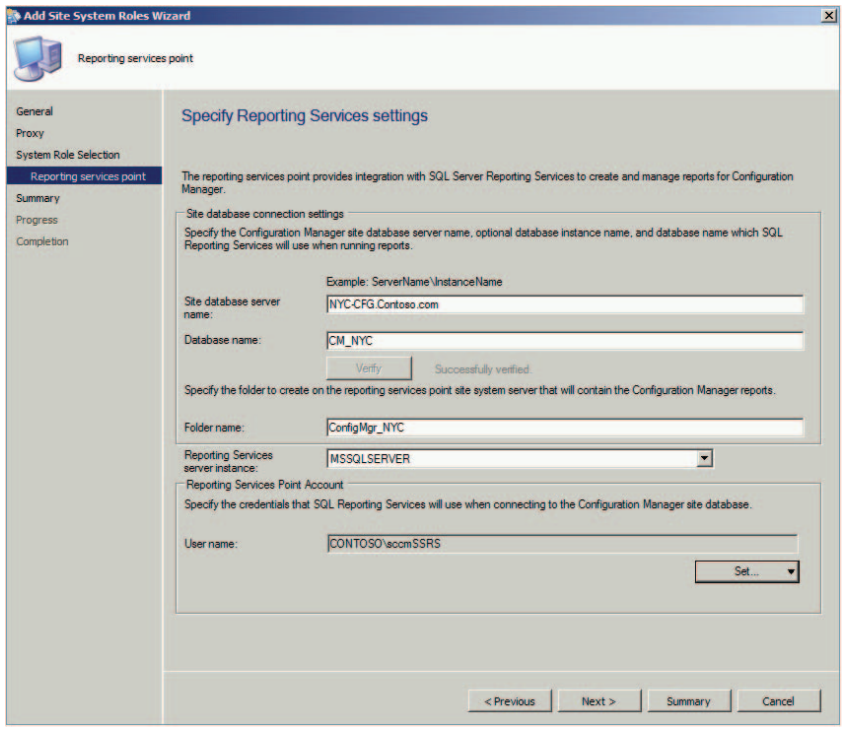


FIGURE 13.1 Creating the data source

12. On the Summary page, verify the settings and click Next.

13. On the Completion page, click Close.

A Few Notes about the Data Source Authentication Account

The data source authentication account is used when Reporting Services retrieves the data for reports from the site database. When you specify the account in the wizard, the installation process will take the account and do the following:

- Assign it the proper SQL permissions.
- Display it as the ConfigMgr SRS reporting point in the Administration workspace, `Accounts` folder.
- Store the account and password encrypted in the Reporting Services database.

What Happens during the Installation?

When the installation begins, Configuration Manager will perform these steps:

1. Create the data source with the specified data source authentication account.
2. Create a root folder for all Configuration Manager reports.
3. Add the ConfigMgr Report Users and ConfigMgr Report Administrators security roles in Reporting Services.
4. Create subfolders and files in `%programfiles%\SMS_SRSRP`.
5. Deploy all reports in the `%programfiles%\SMS_SRSRP\Reports` folder.
6. Assign all user accounts in Configuration Manager the ConfigMgr Report Reader rights on root folders and the Configuration Manager folder.
7. Assign all user accounts with Site Modify rights in Configuration Manager the ConfigMgr Report Administrator rights on root folders and the Configuration Manager folder.
8. Read the current permissions in Configuration Manager, and map those to the newly created reporting folders.
9. Assign users who have Run Report permission for any object ConfigMgr Report Reader rights to the associated report folder.
10. Assign users who have Report Modify rights in Configuration Manager ConfigMgr Report Administrator rights on the associated report folder.
11. Retrieve the mapping between report folders and Configuration Manager secured object types (those maintained in the Configuration Manager site database).
12. Configure the following rights for administrative users in Configuration Manager to specific report folders in Reporting Services:
    - Add users and assign the ConfigMgr Report Users role to the associated report folder for administrative users who have Run Report Permissions for the Configuration Manager object.
    - Add users and assign the ConfigMgr Report Administrators role to the associated report folder for administrative users who have Modify Report permissions for the Configuration Manager object.

Configuration Manager connects to Reporting Services and sets the permissions for users on the Configuration Manager and Reporting Services root folders and specific report folders. After the initial installation of the Reporting Services point, Configuration Manager connects to Reporting Services in a 10-minute interval to verify that the user rights configured on the report folders are the associated rights that are set for Configuration Manager users. When users are added or user rights are modified on the report folder by using Reporting Services Report Manager, Configuration Manager overwrites those changes by using the role-based assignments stored in the site database. Configuration Manager also removes users who do not have Reporting rights in Configuration Manager.

Verifying the Installation

You can verify the Reporting Services installation by monitoring these log files:

sitecomp.log The `sitecomp.log` file will have an entry like this:

```
Starting service SMS_SERVER_BOOTSTRAP_Server with command-line arguments
"SiteCode e:\Program Files\Microsoft Configuration Manager /install➥
E:\Program Files\Microsoft Configuration Manager\bin\x64\rolesetup
.exe➥
SMSSRSRP"
```

srsrpMSI.log `srsrpMSI.log` is the main log file for the installation. You can monitor this for detailed information. Most likely you will find this log file interesting only when troubleshooting a failed installation.

srsrp.log Once the site system is installed, you can monitor the `srsrp.log` file. It gives you detailed information about the folders and reports as they are published to the reporting site.

You can also monitor the folders created in `%ProgramFiles%\SMS_SRSRP`:

Reports Contains all the default RDL files. The reports are imported during the original installation process. You can use the RDL files to import one or multiple reports again.

Resources Contains various DLL files.

Style Contains the three graphical elements used in most reports. You can replace these files with a custom company logo, for example.

The final test is to connect to the reporting site and verify that you can view all of the reports. Open a browser and type **http://reportingserver/reports**. Figure 13.2 shows the items in ConfigMgrReports.

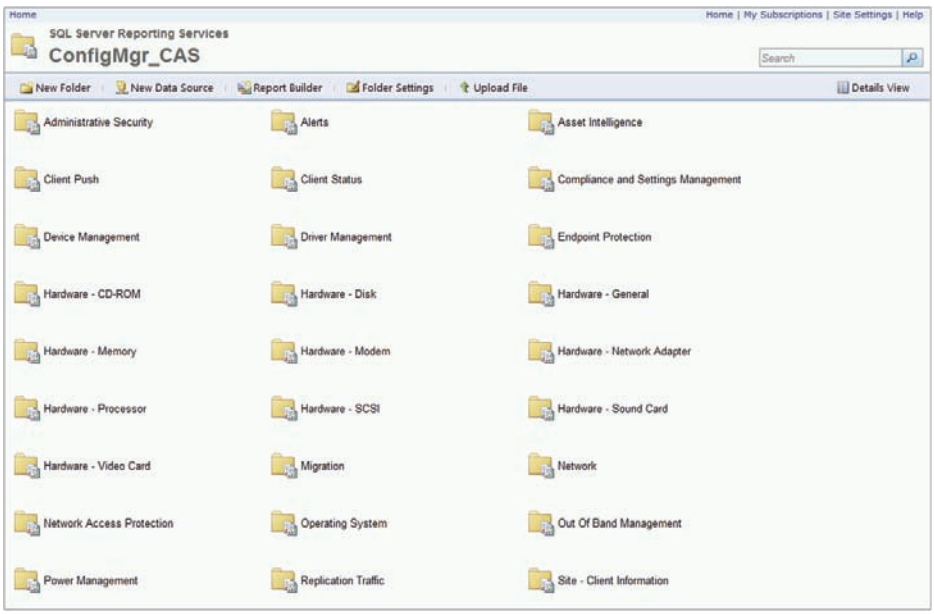


Figure 13.2 Viewing the default reports

Default Reports

By default over 469 canned reports are added during the installation. The reports are organized in several different folders. You can move the reports between the folders as you like and also create new folders. The following folders are available:

Administrative Security Contains information about role-based security, scopes, and audit information.

Alerts Contains information about alerts, such as who closed the alerts.

Asset Intelligence Contains inventory and software license information.

Client Push Contains information about current and past client push installation attempts.

Client Status Contains information about the overall client health and status of the clients installed.

Company Resource Access Contains information about certificate issuance by the certificate registration point and devices/users with certificates about to expire.

Compliance and Settings Management Allows administrators and others to report on Settings Management assignment for a computer or collection. Contain information about the compliance states for computers and collections along with detailed information on configuration items.

Device Management Contains information about device information collected using the Exchange Server mobile connector and from natively managed mobile devices. Integration with Windows Intune provides asset and compliance reporting across cloud-managed PCs as well as mobile devices, including Windows RT, Windows Phone 8, iOS, and Android.

Driver Management Contains information about drivers imported into the drivers repository.

Endpoint Protection Provides detailed information about malware and virus activities. These reports will provide the Security department with up-to-date information about the overall security threat level in the organization.

Hardware – CD-ROM Contains information about CD-ROMs.

Hardware – Disk Contains physical and logical disk information.

Hardware – General Contains a very useful hardware report along with information about the various inventory classes assigned.

Hardware – Memory Contains memory information. You will find information for a specific computer and a count of each unique memory configuration.

Hardware – Modem Contains modem information.

Hardware – Network Adapter Contains network adapter information like IP address, MAC address, and adapter information.

Hardware – Processor Contain processor information.

Hardware – SCSI Contains SCSI information.

Hardware – Sound Card Contains sound card information.

Hardware – Video Card Contains video card information.

Migration Contains information about the migration process from Configuration Manager 2007 to Configuration Manager 2012. Includes migration jobs, migration job status, and other migration reports.

Network Provides information about IP addresses and IP subnets. These reports will give you the number of IP subnets in the network and how many IP addresses you have in each subnet.

Network Access Protection Provides information about NAP rules and computers that have been affected by one or more NAP policies.

Operating System Provides information about operating systems and service packs in the organization.

Out Of Band Management Provides information about managed client systems equipped with Windows Remote Management Technology (WS-MAN).

Power Management Provides power management information like computer activity, energy cost by day, and energy consumption. The information provides the organization with valuable data about the overall power consumption and also how new client power settings have lowered the environmental impact.

Replication Traffic Provides information about database replication throughout the hierarchy.

Site - Client Information Provides information about Configuration Manager client versions, deployments, assignments, communication settings, and out-of-band management configurations.

Site - Discovery and Inventory Information Provides information about client discovery and inventory information. These reports can be very useful when determining the overall client health of the sites.

Site - General Lists computers belonging to a specific Configuration Manager site, and shows when the site status was last updated.

Site - Server Information Lists all site servers and site system roles for a specific site.

Software - Companies and Products One of the primary folders when searching for installed software applications.

Software - Files Provides information based on the software inventory processes.

Software Distribution - Application Monitoring Provides basic and detailed information about application deployment. These reports will provide you with information about computers where requirements or dependencies have not been met, per asset deployment information, application usage, application infrastructure errors, and application compliance.

Software Distribution - Collections Contains information about collections, maintenance windows, and resources belonging to specific collections.

Software Distribution - Content Contains information about distribution points, distribution groups, content, and distribution point usage.

Software Distribution - Package and Program Deployment Contains information about package deployments.

Software Distribution - Package and Program Deployment Status Contains information about statuses for package deployments.

Software Metering When software is enabled, you will use the reports as the primary information source to find information about the applications you monitor, when they were last started and by whom, and where they are installed but not used. The reports will enable you to determine which applications you can uninstall and that way cut down on the license costs.

Software Updates - A Compliance Provides overall compliance information about the software updates released from Windows Updates and also third-party software updates authored and published using the System Center Update Publisher tool.

Software Updates - B Deployment Management Provides information about the software update deployments created in the organization and updates that are required but not yet deployed. You can use the reports in this category to assist you when troubleshooting software update deployments.

Software Updates - C Deployment States This category contains some of the most used reports whenever you work with software update deployment. The single-most important report (in my opinion) is States 1 - Enforcement States for a Deployment. This report can be used to track down the deployment processes of any given software update deployment along with compliance information.

Software Updates - D Scan Reports in this category provide you with information about which clients are able to perform a scan against the WSUS server. The report Scan 1 - Last scan states by collection is the very first report you should run whenever you want to troubleshoot software update problems. If clients are unable to perform a scan, they will not be able to upload compliance information or install required software updates.

Software Updates - E Troubleshooting Contains a few reports that can assist you when troubleshooting client scans and update deployments.

State Migration Provides operating system state migration information for a specific site or state migration site system point.

Status Messages Allows you to see all status messages received by the site server. Useful to determine the health of the Configuration Manager hierarchy.

Status Messages - Audit Allows you to see audit status messages for a specific site or user if using a Configuration Manager agent to remotely control devices.

Task Sequence - Deployment Status Provides you with detailed information about the status of running and historical task sequence deployments.

Task Sequence - Deployments Provides you with detailed information about running and historical task sequence deployments.

Task Sequence - Progress Provides you with detailed information about the progress of task sequences.

Task Sequence - References Provides information about the objects referenced by a specific task sequence.

Upgrade Assessment Provides you with an overview of computers that meet the system requirements for Windows 7 and Windows 8 deployment and those computers that are not capable of being upgraded.

User – Device Affinity Provides you with UDA information, such as UDA associations per collection and UDA statistics.

User Data and Profiles Health Provides you with information about users in a specific domain, a count of users, and computers used by specific users.

Users Provides you with information about users in a specific domain, a count of users, and computers used by specific users.

Virtual Applications Provides information about virtual applications installed in the environment and information about virtual application packages.

Wake On LAN Provides information about the Wake On LAN activity and configurations.

As you can see, Microsoft has done a good job of providing some key reports that are ready to use out of the box.

Running a Report

There are two ways to run a report. The first is to use the Configuration Manager administrative console, and the second is to use the web-based Report Manager. From a management perspective it seems nicer to run the reports from the web-based Report Manager. From here you can also manage and customize the reports.

Viewing Available Reports

You can view the list of available reports from within the Configuration Manager administrative console or through the web-based Report Manager created during the configuration of the Reporting Services site system role. Both Report Manager and Configuration Manager group reports in folders. If needed, you can always move a report from one folder to another folder or even create your own folders.

Running a Report from the Administrative Console

To run a report using the Configuration Manager administrative console, follow these simple steps:

1. Open the Configuration Manager administrative console and select the Monitoring workspace.
2. Under Overview, expand Reporting, select Reports, and choose the reporting category, for example, Client Push.
3. Select the report you want to run, and click Run on the ribbon.

   For example (Figure 13.3), I ran Client Push Installation Status Summary.
4. Many of the reports require that you select additional information, such as a collection, to narrow the search.

   In this example, I clicked Values and selected a value from the Parameter Value window.
5. Click View Report.

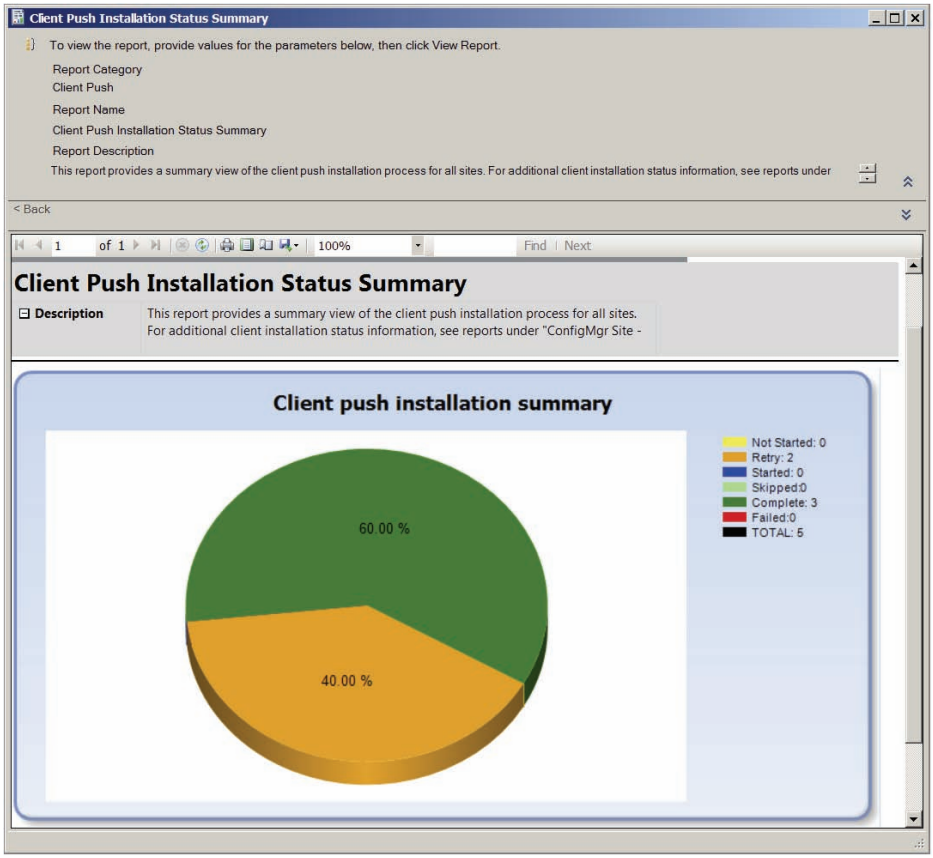


FIGURE 13.3
The Client Push status report opened from the console

This will open the report in a new window. You can choose to print or export the report. If you choose to export the report, you can select a file format like Word, Excel, PDF, TIFF, MHTML, CSV, or XML. A sample report is shown in Figure 13.3, demonstrating some of the available options once you have the report open.

Running a Report from Report Manager

To run a report using the web-based SQL Server Reporting Services, follow these simple steps:

1. Open your web browser to the URL (the default is `http://ReportServer/Reports`) for Report Manager.

   As described earlier in the chapter, this URL is the location you specified when setting up the reporting site system role.

2. Open the folder to the category of the report you want to run.

   In this example, I selected Software Distribution - Application Monitoring.

3. Hover your mouse over the icon in the Report Information area to display the report contents.
4. Select the report you want to run.

   I selected All Application Deployments (Advanced).
5. Again, you will be required to select some criteria from the drop-down boxes.
6. Once you have selected the criteria, click View Report.

   This will display a report, as shown in Figure 13.4.

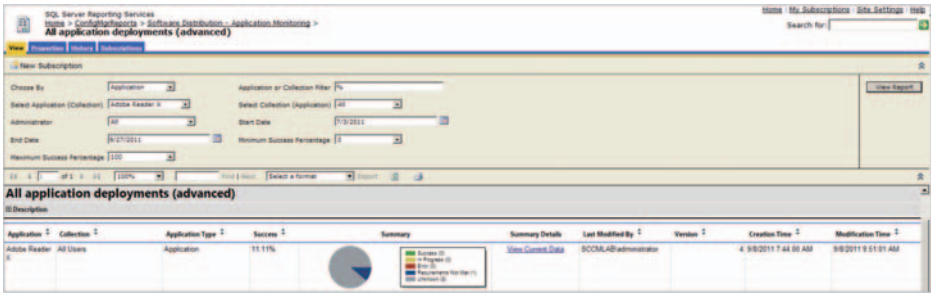


Figure 13.4 Contents of the Software Distribution - Application Monitoring report

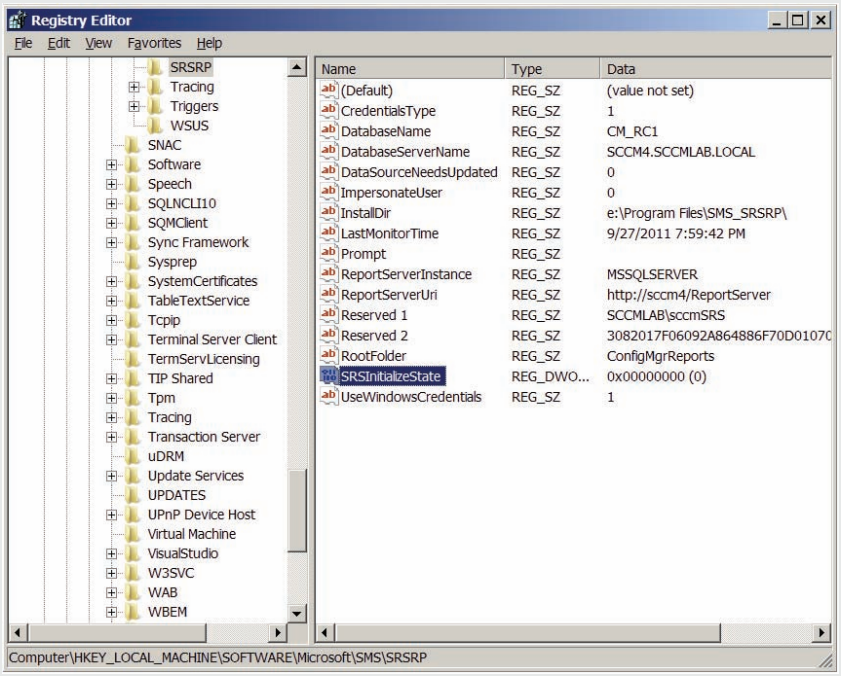


Real World Scenario

Modifying the Standard Logo for All Reports

You have been asked by your boss to make sure that canned SQL reports are branded with the company logo in the upper-right corner. In most canned reports you will find three standard images. You want to replace the `Report_Header_Right.png` file with the custom company logo. To achieve that, you'll use your knowledge of the `Style` folder and make a change in the registry.

1. Log on to the reporting server.
2. Open the `%ProgramFiles%\SMS_SRSRP\style` folder.
3. Make a backup of the existing `Report_Header_Right.png` file.
4. Copy the file of your company's logo to the `Style` folder and rename it **`Report_Header_Right.png`**.
5. Open the registry by clicking Start ➢ Run, and type **`regedit`**.
6. Navigate to `HKEY_Local_Machine\Software\Microsoft\SMS\SRSRP\SRSInitializeState`.
7. Change the value to **`0`**, as shown in the following graphic.



This will restart the deployment of the canned reports. Note that all existing changes to the reports will be overwritten.

It can take a little while for the changes to take effect; you can monitor the `srsrp.log` file on the site server for progress.

Working with Reporting Security

Working with security for reports is not that different from working with security for other objects in Configuration Manager. Configuration Manager will automatically synchronize the security settings configured using the Configuration Manager administrative console to SSRS. In theory you can configure security in both the Configuration Manager administrative console and in Report Manager. The preferred method is using the Configuration Manager administrative console because all changes applied here will automatically be synchronized to SQL Server Reporting Services. If you configure security directly in Report Manager, you will find that all your custom settings will be overwritten by the security settings in Configuration Manager. By default Configuration Manager will connect to SSRS every 10 minutes and verify that security settings are correctly configured.

Permissions Required to Run Reports

Configuration Manager will create two new Reporting security groups in SQL Server Reporting Services:

ConfigMgr Report Administrators Offers full administrative permissions to all tasks related to working with reports.

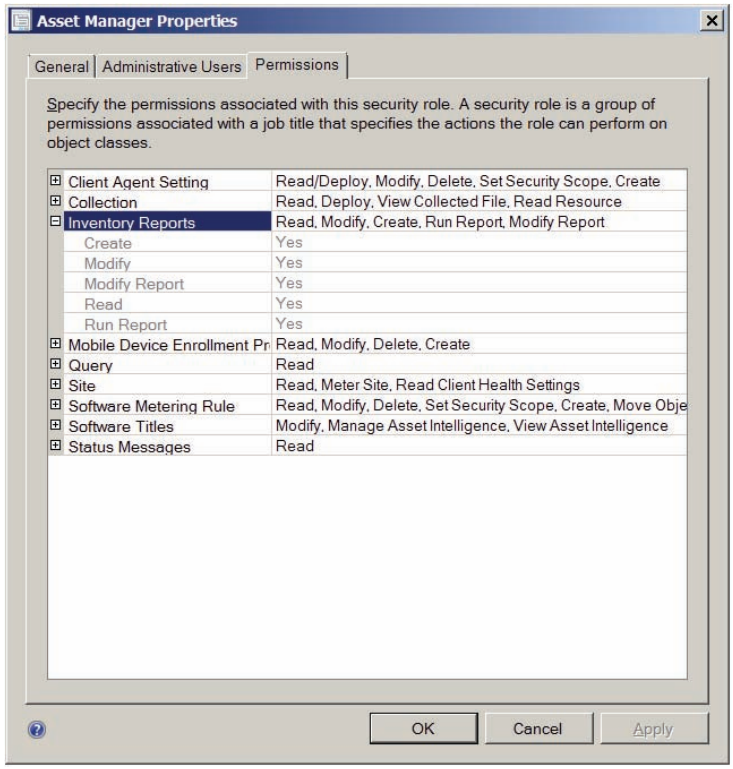


FIGURE 13.5
Report options for built-in security roles

ConfigMgr Report Users Allows users to read reports and create subscriptions.

When you assign the Read permission to a user or group in the Configuration Manager console, that group will automatically be granted the ConfigMgr Report Users role in SQL Server Reporting Services.

Most, but not all, objects will be assigned either Run Report or Modify Report or both, as shown in Figure 13.5, for the Asset Manager. To read reports not associated with a specific role, you must have Read permission to the site. When security is granted, Configuration Manager will automatically assign the appropriate group or user permissions to the reports.

The following list shows the built-in roles and the report folders they can access:

Application Administrator:

- Alerts
- Device Management
- Software Distribution - Application Monitoring
- Software Distribution - Collections
- Software Distribution - Content
- Software Distribution - Package and Program Deployment
- Software Distribution - Package and Program Deployment Status

- User - Device Affinity
- Virtual Applications

Application Author:

- Alerts
- Software Distribution - Application Monitoring
- Software Distribution - Collections
- Software Distribution - Content
- Software Distribution - Package and Program Deployment
- Software Distribution - Package and Program Deployment Status
- Virtual Applications

Application Deployment Manager:

- Alerts
- Software Distribution - Application Monitoring
- Software Distribution - Collections
- Software Distribution - Content
- Software Distribution - Package and Program Deployment
- Software Distribution - Package and Program Deployment Status
- User - Device Affinity
- Virtual Applications

Asset Manager:

- Asset Intelligence
- Hardware - CD-ROM
- Hardware - Disk
- Hardware - General
- Hardware - Memory
- Hardware - Modem
- Hardware - Network Adapter
- Hardware - Processor
- Hardware - SCSI
- Hardware - Sound Card
- Hardware - Video Card
- Operating System

- Site - Discovery and Inventory Information
- Software - Companies and Products
- Software - Files
- Software Metering
- Upgrade Assessment
- Users

Company Resource Access Manager:

- Alerts

Compliance Settings Manager:

- Alerts
- Compliance and Settings Management
- User Data and Profiles Health

Endpoint Protection Manager:

- Alerts
- Endpoint Protection

Full Administrator: All folders

Infrastructure Administrator:

- Alerts
- Asset Intelligence
- Client Push
- Client Status
- Hardware - CD-ROM
- Hardware - Disk
- Hardware - General
- Hardware - Memory
- Hardware - Modem
- Hardware - Network Adapter
- Hardware - Processor
- Hardware - SCSI
- Hardware - Sound Card
- Hardware - Video Card
- Migration

- Network
- Operating System
- Out Of Band Management
- Power Management
- Replication Traffic
- Site - Client Information
- Site - Discovery and Inventory Information
- Site - General
- Site - Server Information
- Software - Companies and Products
- Software - Files
- Status Messages
- Status Messages - Audit
- Upgrade Assessment
- Users
- Wake On LAN

Operating System Deployment Manager:

- Alerts
- Driver Management
- Software Distribution - Application Monitoring
- Software Distribution - Collections
- Software Distribution - Content
- Software Distribution - Package and Program Deployment
- Software Distribution - Package and Program Deployment Status
- State Migration
- Task Sequence - Deployment Status
- Task Sequence - Deployments
- Task Sequence - Progress
- Task Sequence - References
- Virtual Applications

Operations Administrator: All folders

Read-only Analyst: All folders

Remote Tools Operator: No folder view

Security Administrator:

- `Administrative Security`

Software Update Manager:

- `Alerts`
- `Hardware – General`
- `Network Access Protection`
- `Software Updates – A Compliance`
- `Software Updates – B Deployment Management`
- `Software Updates – C Deployment States`
- `Software Updates – D Scan`
- `Software Updates – E Troubleshooting`



Real World Scenario

Assign a Group Permission to View All Reports

In your organization you have an Active Directory group named CM_Reporting_Viewers that requires read access to all reports in Configuration Manager. As a Configuration Manager administrator you have been assigned the task of assigning the appropriate permissions using the least administrative effort possible. Follow these steps to accomplish this task:

1. Open the Configuration Manager administrative console.
2. Navigate to the Administration workspace, and in Overview select Security ➢ Administrative Users.
3. From the ribbon click Add User Or Group.

   This will launch the Add User Or Group dialog.
4. In User Or Group Name field, click Browse, type **CM_Reporting_Viewers**, and click OK.
5. In the Associated Security Roles dialog, click Add, select the Read-only Analyst security role, and click OK.
6. Click OK to close the Add User Or Group dialog.

Managing Reports

One of the main benefits of using SQL Server Reporting Services is the ability to manage reports. Once a report is published, you will be able to use the Report Manager to modify some of the reporting properties. Properties control security, parameter values, the data source, when the report runs (scheduled or on demand), caching options, and more.

To manage the properties for a report, follow these simple steps:

1. Open your web browser to the URL (the default is `http://ReportServer/Reports`) for the Report Viewer.
2. Open the folder to the category of the report you want to manage, for example, Software Distribution - Application.
3. Click the drop-down arrow for the report you want to manage.
4. From the list of options, click Manage.

The first properties you will see are the General properties for the report. You will find a list of report properties in Tables 13.1 through 13.9. Table 13.1 lists the General properties.

TABLE 13.1: General properties

PROPERTY	DESCRIPTION
Delete	Allows you to delete the report.
Move	Allows you to move the report to another folder. This is especially useful if you want to create your own folder with a mix of canned reports from different folders. You should always consider creating custom folders like `Servicedesk`, `Software`, or `License` and move the reports you use the most to those folders.
Create Linked Report	Allows you to create a link to another report. You will find more information on this property later in this chapter.
Download	Allows you to save the report as an RDL file.
Replace	Allows you to import a new version of the report.
Name	Lets you specify the name of the report.
Description	Lets you provide the report description.
Hide In Tile View	Enable this to hide the report from the Report Manager tile view mode. Tile view mode is the default view when users browse for reports.

SHOWING HIDDEN REPORTS IN REPORT MANAGER

To view a report that is configured to be hidden in List view, do the following:

1. Open the Report Manager website.
2. Click Details View.
3. Open the folder containing the report you want to view.
4. In Details view all reports and data sources are visible. You can now open the specific report's properties and remove the check mark from Hide In Tile View on the General properties page.

Reimport a Canned Report

As you start working with reports, you might find yourself modifying reports and later regretting it. All canned reports that are installed with Configuration Manager are located in a folder on the reporting site system. In this example we will reimport the Client Status Summary report from the `Client Health` folder. To manually import this report, do the following.

1. Open the Report Manager website.
2. Open the `Client Health` folder.
3. Open the Client Summary report properties, and make sure you are on the General properties page.
4. Click Replace.
5. Click Browse and navigate to `E:\Program Files\SMS_SRSRP\Reports\Client_Health`, where `E:\` is the disk volume where you have installed the reporting site system role.
6. Select `CH_Report_ClientSummaryCurrent.rdl` and click Open.
7. Back in Report Manager, click OK.
8. Click Apply and close the report properties.

Using prompts (or parameters) in reports is very common. It is an easy way for the report user to specify what data to view without having to have deep knowledge of the underlying dataset or SQL reporting skills. You as the administrator can customize the parameters and configure settings such as the default parameter values described in Table 13.2.

Table 13.2: Parameter properties

Property	Description
Parameter Name	The name of the parameter.
Data Type	Specification of the data type.
Has Default	Allows you to specify a default value, thus saving time whenever you run the report. With this selected you can specify the value in Default Value and/or use the Null property.
Default Value	A default value can originate from the report definition, can be query based, or can be a value you type in. The value you enter must adhere to the data type; the use of wildcards is also determined in the report itself.
Null	Allows you to specify that the report will run even if the user does not select any prompted value. This does require that the report allows the use of Null values.
Hide	Allows you to hide the parameters in the Report Manager from users when they run a report. The parameter value will still be visible if the user starts the subscription wizard.
Prompt User	With this selected, users will be prompted for a parameter. Deselect the check box if you want to control the parameters to be used in the report.
Display Text	Text that will be displayed with the parameter value.

As part of the SQL Server Reporting Services point installation, a shared data source is created. The data source is used to specify what data to access and which security credentials to use. Table 13.3 describes the values you can specify for the created data source. Notice that it is highly unlikely that you will need to change the data source from the Report Manager.

TABLE 13.3: Data Source properties

PROPERTY	DESCRIPTION
A Shared Data Source	Specifies the shared data source.
A Custom Data Source	Allows you to specify a custom data source.
Connection String	Specifies the connection string used to connect to the data source.
Connect Using	Defines how you connect to the data source. For all the canned reports, the connection settings are already defined in the connection string.
Connect Using Credentials Supplied By The User Running The Report	Defines that each user must provide a username and password.
Use As Windows Credentials When Connecting To The Data Source	Configure this option if the credentials supplied by the user are Windows Authentication credentials.
Credentials Stored Securely In The Report Server	Encrypts and stores the credentials in the report server. This will allow you to run a report unattended, which is a requirement for scheduled reports.
Impersonate The Authenticated User After A Connection Has Been Made To The Data Source	Used only in rare occasions to allow delegation of credentials if supported by the data source.
Windows Integrated Security	Uses the credentials of the logged-on user to access the data source.
Credentials Are Not Required	Does not prompt for credentials when running the report. This works only if the data source does not require a user logon.
Test Connection	Performs a test to the data source using the supplied credentials.

One of the advantages of using SQL Server Reporting Services is that you can configure automatic delivery of specified reports by either email or storing the report to a file share. You can create subscriptions in the Report Manager or using the Create Subscription Wizard in the Configuration Manager administrative console. Table 13.4 explains the subscription options available when you are using the Report Manager.

Table 13.4: Subscription options

Property	Description
New Subscription	Allows you to create a new report subscription.
Delete	Lets you delete the selected subscription.
Edit	Allows you to edit the subscription properties.
Report Delivery Options (email Selected)	Can be delivered by email or can be file based. Following are the properties for an email-based subscription.
To	Fill in the recipient email address; it can be a group or a list of individual email addresses separated by a semicolon (;). Note that the reporting server will not validate any of the email addresses.
Cc	Fill in the email address of any recipients who will receive the email as Cc. Can be a group or a list of individual email addresses separated by a semicolon.
Bcc	Fill in the email address of any recipients who will receive the email as Bcc. Can be a group or a list of individual email addresses separated by a semicolon.
Reply-To	Fill in the Reply To email address.
Subject	The email subject; you can use these variables combined with custom text: *@ExecutionTime*—The run time for the report *@ReportName*—The name of the report
Include Report	Includes the report in the email as an attachment.
Render Format	Reports can be delivered in different formats: XML CSV (comma delimited) Data Feed PDF HTML 4.0 MHTML (MIME HTML) Excel RPL Renderer (RPL) TIFF File Word
Include Link	Includes a URL in the email body.
Priority	Choose from these email priorities: Low Medium High

TABLE 13.4 Subscription options *(CONTINUED)*

Property	Description
Comment	Text entered in the comment will be added to the email body.
Report Delivery Options (Windows File Share)	Following are the properties for Windows file share subscription.
File Name	Type in the filename of the report.
Add A File Extension When The File Is Created	By default the file type will not be appended to the filename unless you enable this setting.
Path	A UNC to an existing folder on the network. The specified user account must have Write permissions to the share.
Render Format	Same as the email rendering formats.
Credentials Used To Access The File Share	Specify the user account that will be used to save the file.
Overwrite Options	Choose from these options: Overwrite An Existing File With A Newer Version. Do Not Overwrite An Existing File. Increment File Names As Newer Versions Are Added. This will place a number at the end of the filename and increment the number as new reports are saved.

When reports are executed, they will be transformed from the reporting database into a viewable format. The defined query in the dataset will be executed and will return data to the reporting server, where the selected rendering extension will create the report. The performance impact of running a report depends very much on the amount of data retrieved and the rendering format selected. By default when users run a report, that report is generated on demand. Most of the data in Configuration Manager is either inventory data or state messages, which are very rarely real-time data. By knowing the processing options described in Table 13.5 and the report content, you will quickly learn how to speed up the processing for reports.

When you cache a report, the first time the report is executed the process is similar to running an on-demand report. However, the intermediate format is stored in ReportServerTempDB (cache) for a configured period. If any other users request the same data, the server will take the intermediate format and render the report much more quickly.

TABLE 13.5: Processing options

Property	Description
Always Run This Report With The Most Recent Data.	Always shows the latest data in the report.
Cache A Temporary Copy Of The Report. Expire Copy Of Report After A Number Of Minutes.	Specifies the number of minutes the intermediate format will be available in the cache.

Property	Description
Cache A Temporary Copy Of The Report. Expire Copy Of Report On The Following Schedule.	You can specify when the intermediate format will be removed from the cache based on a custom specific schedule or by using a shared schedule.
Render This Report From A Snapshot.	This option allows you to create the intermediate format prior to running the report the first time. The intermediate format can be created on a custom specific schedule or by using a shared schedule. Note that cached reports will be added as permanent storage to the ReportServer database, unlike cached reports, which will be removed. This feature is closely related to the values you specify on the Snapshot Options page.
Create A Report Snapshot When You Click The Apply Button On This Page.	Creates a snapshot of the report as soon as possible without using the specified schedule.
Report Timeout.	Controls the report processing timeout value. The default timeout value is specified in the Site Settings page.

You can preload the cache with temporary copies of the report by creating a refresh plan with the parameters described in Table 13.6. Creating a cache refresh plan requires that the cache options have been defined.

Table 13.6: Cache Refresh options

Property	Description
New Cache Refresh Plan	Lets you create a new plan.
Description	You can provide a meaningful description for the plan.
Refresh The Cache According To The Following Schedule	The cache can be refreshed on a custom specific schedule or by using a shared schedule.

As snapshots are generated, you will be able to view the reports in the Report History page. On this page you can also create a manual snapshot of the report. The options are shown in Table 13.7.

Table 13.7: Report History options

Property	Description
Delete	Deletes the selected report snapshot.
New Snapshot	Creates a new snapshot. This option is available only if Allow Report History To Be Created Manually has been selected on the Snapshot Options page.

Report history is stored in the Report Server database. The Snapshot options, shown in Table 13.8, will assist you in controlling how many items are stored and when the snapshot is generated.

TABLE 13.8: Snapshot options

PROPERTY	DESCRIPTION
Allow Report History To Be Created Manually	Enables the New Snapshot button on the Report History page.
Store All Report Execution Snapshots In Report History	With this feature, reports that are created based on the execution settings on the Processing Options page will be added to the Report History page.
Select The Number Of Snapshots To Keep	Controls how many snapshots are added to the history. You can select from three different values: Use Default Unlimited Snapshots Limit To A Specific Number

As described earlier in this chapter, Configuration Manager will apply default security settings when the Reporting Services point is installed and will check those security settings every 10 minutes. Table 13.9 describes the Security setting applied to a report.

TABLE 13.9: Security option

PROPERTY	DESCRIPTION
Edit Item Security	Allows you to customize the default Security settings. Notice that Configuration Manager will overwrite any custom settings you configure.

CREATING A SHARED SCHEDULE

To lower the performance requirements on the server when running reports, you have been asked to control when reports are rendered. Prior to configuring the execution options, you decide to create a shared schedule that can be selected for all reports. You follow these steps to create a shared schedule:

1. Open the Report Manager website.
2. Click Site Settings.
3. Click the Schedules link.
4. Click New Schedule.
5. Type in a schedule name and configure the schedule details.
6. Click OK to save the shared schedule.

Working with Subscriptions

One of the many features of using SQL Server Reporting Services is working with subscriptions. You can subscribe to reports and have them delivered via mail or as a file on a network share. A standard user can create and customize their own subscriptions with the options described in Table 13.4. You can create a subscription in Report Manager or use the Create Subscription Wizard in the Configuration Manager administrative console.

Creating a File-Based Report Subscription

Prior to creating a file-based subscription, you need to ensure that you have an account with write permissions to a predefined server share. In this example we'll create a subscription for the Client Push Status Summary report.

To create a file-based report subscription using the Configuration Manager administrative console, follow these steps:

1. Open the Configuration Manager console and select the Monitoring workspace.
2. Inside Overview, click Reporting, and select the report from the `Reports` folder.
3. With the report selected, click Create Subscription on the ribbon.
4. In the Report Delivered By field, ensure that Windows File Share is selected.
5. In File Name field, type in the name of the file without any extension, for example, **`ClientPushSummary`**.
6. Enable the Add File Extension When Created check box.
7. In the Path field, type in the UNC to an existing share.
8. Select the rendering format; in the example I have selected Acrobat (PDF) File.
9. In the User Name field, specify an account with Read access to the report and Write permissions to the specified UNC.
10. Configure the needed Overwrite Option, and click Next.

    Figure 13.6 shows how the delivery options can be specified.
11. On the Subscription Schedule page, select a shared schedule or create a new schedule, and click Next.

    This report is a prompted report, and it requires that you select the prompted value. In this example you must click Values and select the number of days.
12. Select All, click OK, and click Next.
13. Read the summary information, and click Next.
14. Click Close; the subscription is now created.

You can view information and edit the scheduled report by clicking Reporting ➢ Subscriptions in the Monitoring workspace. You can also open the Report Manager and open the properties for the report. Select Subscriptions; here you will find detailed information about when the subscription is about to run or when it was executed the last time.

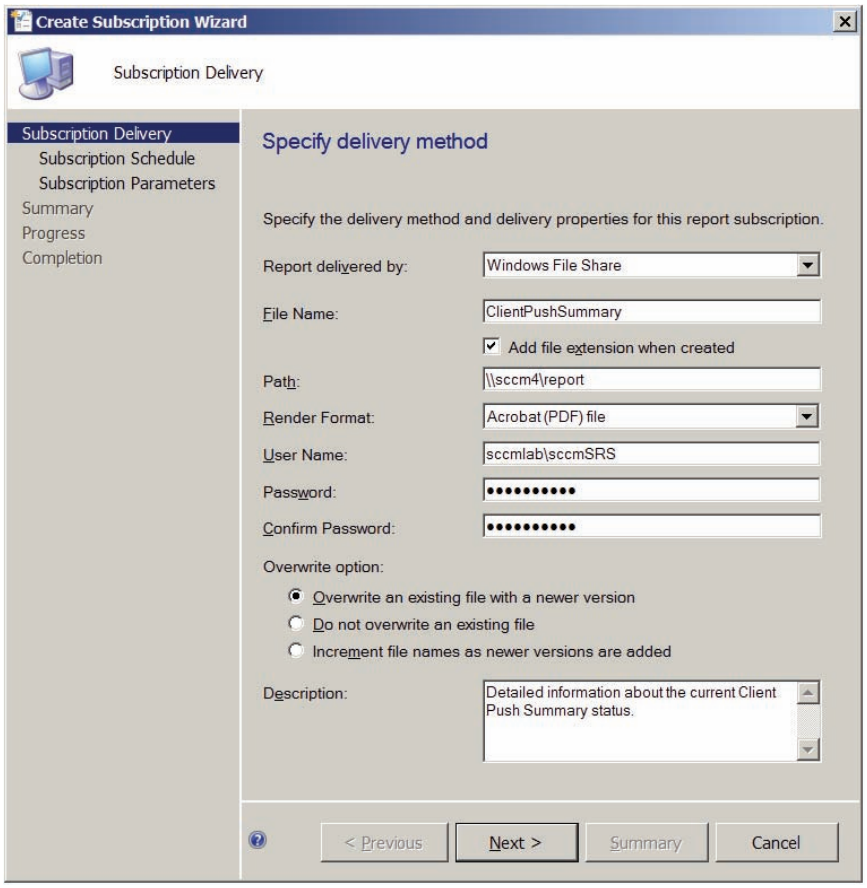


Figure 13.6
Creating a Windows file-based report subscription

Creating an Email-Based Report Subscription

Prior to creating an email-based subscription, you need to configure the email options in the Reporting Services Configuration Manager. In this example you will configure the required mail options and use Report Manager to create a subscription for the Client Push Status Summary report.

To configure email support in the Reporting Services Configuration Manager and create an email-based subscription in Report Manager, follow these steps:

1. From the Start menu, choose All Programs ➢ Microsoft SQL Server 2008 R2 ➢ Configuration Tools ➢ Reporting Services Configuration Manager.
2. You will be prompted to connect to a reporting server. Make sure the correct reporting server and instance are selected and click Connect.
3. Click E-Mail Settings.
4. In Sender Address, type the email address that will be used to send the mail.
5. In Current SMTP Delivery Method, ensure that Use SMPT Server is selected.

6. In SMTP Server, type the name of the SMTP server and click Apply to store the settings.
7. Click Exit to close the Reporting Services Configuration Manager.
8. Open the SQL Report Manager and connect to the Configuration Manager report by typing **`http://reportingserver/reports`**.
9. Open the `Configuration Manager` folder and the `Client Push` folder.
10. Hover the mouse over the report, and select Subscribe from the drop-down list.
11. In Delivered By, ensure that E-Mail is selected.
12. In To, type the recipient email addresses.

    Note that there will be no validation of the addresses; you need to make sure that what you type is correct. You can type multiple addresses by separating them with a semicolon (;).
13. Fill in any other CC, BCC, and Reply-To email addresses.
14. Type a subject using the variables explained in Table 13.4.
15. Choose from among the following options:
    - Send A Link
    - Include The Report As Attachment
    - Embed The Report In The Mail

    If the recipients support HTLM 4.0 and MHTML 5.0, you can select the Render format MHTML; this will embed the report in the mail.
16. In the Comment field, type in any information that you want to include in the mail body.
17. Configure the processing options, and click OK to create the subscription.

You can create the subscription in Report Manager as explained previously or in the Configuration Manager administrative console as explained for file-based subscription. The difference between the two methods is that subscriptions created in the administrative console will be listed in the administrative console as well as in Report Manager, unlike subscriptions created in Report Manager, which will be listed only in Report Manager.

Creating Reports

Even though Configuration Manager 2012 SP1 ships with over 469 canned reports, a few of which are hidden, at some point you will need to modify an existing report or create a new one. Creating reports requires that you have a basic understanding of SQL and that you are familiar with the different tools available to customize reports. In essence you can create a new report in the following ways:

- From scratch using Report Builder or BIDS (Business Intelligent Development Studio)
- By copying and modifying an existing report
- By creating a new report based on a report model

When you create reports, you will use data stored in the site server database through SQL *views*. SQL views are essentially virtual tables that do not themselves contain any data but are based on tables that contain data. The data is dynamically compiled from source tables when the view is referenced. It is not recommended to query tables directly because tables can be changed, for example, by installing a Configuration Manager service pack. Once you know the basics of the naming standard used for views, they actually start to make sense:

- V_GS_Name—Contains current inventory data
- V_HS_Name—Contains history inventory data
- V_R_Name—Contains discovery data
- V_RA_Name—Contains array (multivalue) discovery data

Basic SQL Commands

So far in the chapter you've seen how to create a new report using SQL Report Builder and how to import a report. The other option is to define the report using SQL scripting. This, of course, requires you to know the relevant SQL commands. In general, an understanding of SQL syntax is a huge asset for a Configuration Manager administrator but not a requirement. However, within the scope of this book, we cannot cover SQL commands in depth. We suggest that you read up on basic SQL commands so you can create rich and powerful reports. Another way to learn is by simply opening existing reports and seeing how they are written.

Although we cannot cover every topic within SQL programming, such as how to define queries to achieve rich reports within Configuration Manager, it will be useful to cover basics such as `ORDER BY`, sorting with `DESC` and `ASC`, `COUNT`, and setting header names using `AS`.

For all the examples we will be using the same report statement, shown here:

```
SELECT
count(model0) as Count, Model0 as 'Computer Model', Manufacturer0 as
'Manufacturer'
FROMv_GS_COMPUTER_SYSTEM GROUP BY Model0, Manufacturer0
ORDER BY count DESC
```

The result of the statement would look similar to the following output:

```
Count        Computer Model        Manufacturer
5            Virtual Machine       Microsoft Corporation
```

One way to make the presentation of reports look professional is to sort the items in some fashion. Within SQL you can use a command such as the following to sort your reports:

```
ORDER BY count DESC
```

`ORDER BY` is the command that tells SQL to sort based on the column `COUNT` in this example. The order in which the items will be sorted is `DESC`, or descending. You can use `ASC` to sort in ascending order.

If you want to sort on multiple items, just add them to the list in the order in which you want to sort, for example:

```
ORDER BY count, Model0 DESC
```

Many times you will be tasked with showing very concise reports in which the end user just wants to know, "How many units of model X do we have in our organization?" This is easily achieved by using the `COUNT` command.

```
SELECT count(model0)
```

This will show the count of the item `Model0` in your report.

Many times, you will not want to have a report with column headings such as `Model0`, `Manufacturer0`, and so on. You will want to display meaningful header names. So the following example shows how to achieve this naming:

```
SELECT
count(model0) as Count, Model0 as 'Computer Model', Manufacturer0 as
'Manufacturer'
FROM v_GS_COMPUTER_SYSTEM
GROUP BY Model0, Manufacturer0
ORDER BY count DESC
```

By adding the word `AS` into your SQL statement, you can specify the name of the column header. If the name contains a space, then you have to use single quotes.

Report Models

A report model contains predefined views and fields logically grouped together. By using report models you can assist users in building reports that expose only the needed views and fields. This shortens the learning curve for building reports and also speeds up the process because only the selected views and fields will be presented to Report Builder. Later in this chapter you will learn how to build your own report model and create reports based on the canned Configuration Manager report models. Some of the benefits of using report models are these:

- You can assign reporting model logical names.
- The underlying database structure can be hidden from the person creating the report.
- The report model can contain multiple tables and views yet still list the model as a single object.
- Time saved is money saved. When reporting models are created, not every person creating reports needs to have deep SQL knowledge.

Creating a Report Using Report Builder

Configuration Manager 2012 uses Microsoft SQL Server 2008 Reporting Services Report Builder 2.0 as the authoring and editing tool for both model and SQL-based reports. SQL Server 2008 R2 ships with a new version of SQL Reporting Builder 3.0, which is an updated version of the version that ships with SQL Server 2008. Report Builder will automatically be installed on your computer when you create or modify a report for the first time. Report Builder has a lower learning curve than BIDS and is often used by non-SQL experts to create custom reports. The tool is not a full-blown developer tool but still offers the support needed by many, such as the following:

- Developing one report at a time in a Microsoft Office lookalike environment
- Creating charts and gauges
- Creating rich SQL
- Rich formatting capabilities
- Exporting to reports in other formats

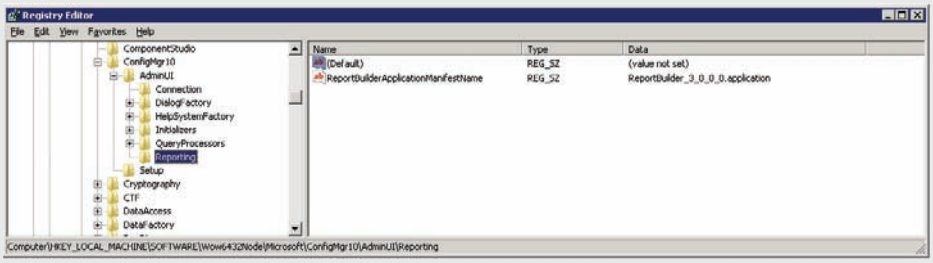


Real World Scenario

Change registry to launch Report Builder 3.0 instead of Report Builder 2.0

You have been asked to modify some of the canned reports using Report Builder 3.0. ConfigMgr 2012 may launch Report Builder 2.0 unless you modify the registry, as follows:

1. Log on to the computer where you have the ConfigMgr 2012 administrator installed.
2. Click Start ➢ Run and type **`Regedit`** to launch the registry editor.
3. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\ConfigMgr10\AdminUI\Reporting`.
4. Modify the `ReportBuilderApplicationManifestName` key, and change the string to **`ReportBuilder_3_0_0_0.application`**, as shown here.



5. Click OK and close the registry editor.

Next, you will see how to create a report using Report Builder 3.0. The report will be created in the report folder called `Hardware - General`. Use the following steps to create a basic SQL report that will show and count all the different hardware models you have in the database.

1. Open the Configuration Manager console and select the Monitoring workspace.
2. In Overview, expand Reporting and right-click Reports.
3. From the drop-down menu click Create Report.
4. Select SQL-based Report.
5. In the Name field type **Count Hardware Models**.
6. In the Description field type **Group and count all hardware models**.
7. In the Path field, click Browse, select the `Hardware - General` folder, and click OK.
8. Click Next.
9. On the Summary page click Next (this will create the report).

10. Click Close.

    Report Builder will launch automatically. If this is the first time you launched the wizard, you will be prompted to install Report Builder.

11. In Report Builder click Table Or Matrix.

    This will launch the New Table Or Matrix Wizard.

12. Click Create A Dataset and click Next.

13. In Data Source Connections, verify that the Configuration Manager data source is selected, and click Next.

14. Expand dbo ➢ Views ➢ v_GS_COMPUTER_SYSTEM.

15. Select Manufacturer0 and Model0, as shown in Figure 13.7, and click Next.

16. Drag Manufacturer0 and Model0 to Row Groups and Model0 to Values.

17. In Values, right-click Model0 and select Count; click Next when finished.

18. In Choose The Layout, select Stepped Subtotals Above, and click Next.

19. Select a style and click Finish.

    The report is now open in Design view, allowing you to customize colors, fonts, and much more.

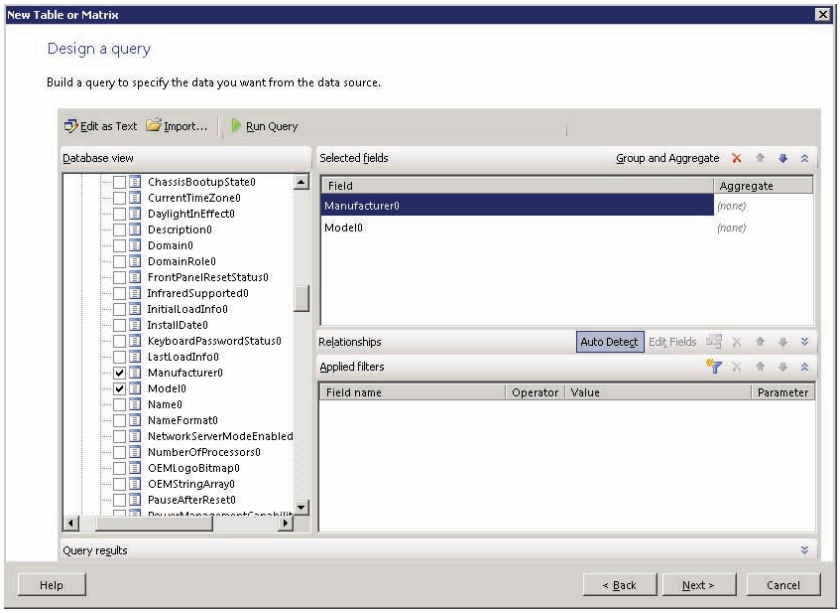


FIGURE 13.7
Creating a report using Report Builder 3.0

20. To view the report, click Run from the ribbon.
21. Click Save to save the report.
22. Exit Report Builder.
23. When prompted to publish the report, click Yes.

Adding a Custom Logo to an Existing Report

You have been asked by management to modify the canned report Enforcement States for a deployment from the `Software Updates` folder. Follow this process to modify the report:

1. Open the Configuration Manager console and select the Monitoring workspace.
2. Expand Overview ➢ Reporting ➢ Reports ➢ Software Updates - C Deployment States.
3. Select States 1 - Enforcement States for a deployment, and click Edit on the ribbon. This will launch the SQL Server Report Builder.
4. From the Report Data column on the left, right-click Images, and select Add Image.
5. Locate the image file and click Open.
6. Drag and drop the image object into the report header.
7. Click OK in the Image Properties dialog.

Creating a Report Using Business Intelligence Development Studio

Business Intelligence Development Studio, or BIDS, is often used by developers when creating more advanced reports. BIDS is a component that ships with SQL Server and is in essence Microsoft Visual Studio 2008 with prebuilt project types used in SQL-like reporting services. BIDS can be installed on SQL Server as well as on a workstation operating system like Windows 7. The following example demonstrates how you can create and publish a report using BIDS. The report will list and count Adobe applications installed on all workstations.

1. Click Start ➢ All Programs ➢ Microsoft SQL Server 2008 R2 ➢ SQL Server Business Intelligence Studio.
2. Select File ➢ New ➢ Project.
3. Select Report Server Project Wizard.
4. Enter the name as **Mastering CM2012**, and click OK.

   This will start a wizard to take you through the process of creating the report.
5. In the Welcome To The Report Wizard dialog, click Next.
6. In Select The Data Source under Name, type **CM2012** and click Edit.
7. In Connection Properties, type the name of the SQL Server in the Server Name field, and select the Configuration Manager database from the Select Or Enter A Database Name drop-down list.

8. Click OK to save the connection properties.
9. Click Make This A Shared Data Source, and click Next.

   In the design query step you can either paste an existing SQL statement or click Query Builder and create your own statement. In this example you will build the statement yourself.
10. Click Query Builder.
11. Click the Add Table icon in the toolbar.
12. Select the Views tab, navigate to V_R_System, and click Add.
13. Select V_GS_ADD_REMOVE_PROGRAMS, click Add, and click Close.
14. Back in Query Designer, arrange the two views so you can see both.
15. From V_R_SYSTEM, drag ResourceID and drop the field on ResourceID in the V_GS_ADD_REMOVE_PROGRAMS view.

    By doing so, you are creating an inner join between the two views. You should see a SQL statement like this:

    ```
    SELECT *
    FROM  v_GS_ADD_REMOVE_PROGRAMS
    INNER JOIN v_R_System ON v_GS_ADD_REMOVE_PROGRAMS.ResourceID =
    v_R_System.ResourceID
    ```

16. From V_GS_ADD_REMOVE_PROGRAMS, select DisplayName0, Publisher0, and Version0.
17. In Publisher0 Filter, type **Like Adobe%**.

    This will ensure that you see only the application from a specific vendor.
18. From V_R_System, select Operating_System_Name_and0.
19. In Filter, type **like %workstation%**, and remove the check mark from Output.

    This will query for all workstations but not show the operating system information in the report.
20. From V_GS_ADD_REMOVE_PROGRAMS, drag DisplayName0 down to the fourth field in your query.
21. In the Alias field, type **Total**.

    You can use the Alias column to type a more descriptive title for each of the fields.
22. To calculate the number of applications installed, click the Use Group By icon on the toolbar.

    Notice that this will add an extra column named Group By.
23. In the last column with DisplayName0, change Group By to Count.

24. Click the red exclamation mark to run the query.

    Your query should look like this (notice that I have used some aliases not mentioned in the previous steps):

```
SELECT
v_GS_ADD_REMOVE_PROGRAMS.DisplayName0 AS Application,
v_GS_ADD_REMOVE_PROGRAMS.Publisher0 AS Publisher,
v_GS_ADD_REMOVE_PROGRAMS.Version0 AS Version,
COUNT(v_GS_ADD_REMOVE_PROGRAMS.DisplayName0) AS Total
FROM  v_GS_ADD_REMOVE_PROGRAMS
INNER JOIN v_R_System ON v_GS_ADD_REMOVE_PROGRAMS.ResourceID =
v_R_System.ResourceID
GROUP BY v_GS_ADD_REMOVE_PROGRAMS.DisplayName0,
v_GS_ADD_REMOVE_PROGRAMS.Publisher0,
v_GS_ADD_REMOVE_PROGRAMS.Version0,
v_R_System.Operating_System_Name_and0
HAVING (v_R_System.Operating_System_Name_and0 LIKE '%workstation%')
AND (v_GS_ADD_REMOVE_PROGRAMS.Publisher0 LIKE 'Adobe%')
```

25. Click OK to close Query Designer.

26. In the Report Wizard, on the Design The Query screen, click Next.

27. In Select The Report Type, ensure Tabular is selected and click Next.

28. In Design The Table, move all available fields to the Details section and click Next.

29. In Choose The Table Style, select Corporate and click Next.

30. In Choose The Deployment Location, verify that the correct SQL report server version and report server are selected.

    The `Deployment` folder will be the location where SQL Server Reporting Services will publish the report. It is often a good idea to publish reports to a "sandbox" folder before adding the report to the same folder as the canned Configuration Manager reports.

31. Click Next.

32. On the Completing The Wizard page, type **Number of Adobe applications installed**.

33. Click Finish.

    Your report is now ready to be customized. You will find many of the features in BIDS that you have in Report Builder to create a fancy report.

    Once you have finished modifying the report, you can deploy the report to the sandbox folder.

34. From the Build menu, select Deploy Mastering CM2012.

Moving Reports

When you are satisfied with the newly created report, you can move it from the sandbox folder to the folder where you have the canned Configuration Manager reports, as follows:

1. Open a browser and connect to `http://reportingserver/reports`.
2. Open the sandbox folder.
3. Click Details View from the toolbar.
4. Select the report and click Move from the toolbar.
5. Browse to the destination folder containing the canned Configuration Manager reports.
6. Click OK, and the report will be moved to the new location.
7. Open the report properties and select Data Source.
8. Browse to the folder containing the canned Configuration Manager reports, and select the shared data source.
9. Click OK.
10. Click Apply.

Linked Reports

A linked report is something you can create when you want to have several versions of the same report with different data. You can look at linked reports as you would cloning an existing report with the exception that a linked report inherits the layout and data source properties of the original report. Properties like parameters, subscriptions, and schedules can be changed in the linked report.



Real World Scenario

Providing Different Teams with the Same Report but Different Data

You need to provide managers from the desktop and server team with a monthly third-party software license reconciliation report in their mailbox. The managers need the same report but with data from different collections. From time to time, you have modified the layout of the report, and you do not want to do that on multiple reports. To meet the challenge you decide to create two linked reports derived from the canned report License 15A - General License Reconciliation Report. Here's how you create the first linked report:

1. Open a browser and connect to `http://reportingserver/reports`.
2. Open the `Asset Intelligence` folder.
3. Click the drop-down arrow for the report License 15A - General License Reconciliation.
4. Select Create Linked Report; notice that you can also do the same thing by opening the report properties.
5. Type a descriptive name for the linked report like **License 15A - Server License Reconciliation Report**.

6. Click OK.
7. Open the properties for the new linked report (notice that by default you still have the properties for the original report open).
8. Select Parameters.
9. Check Has Default, and type the Collection ID in the Default Value field. You can find the Collection ID by viewing the collection properties in the Configuration Manager administrative console.
10. Check Hide, and remove the check mark from Prompt User.
11. Click Apply, and run the report.

Importing and Exporting Reports

One of the fastest and easiest ways to build reports into your Configuration Manager console is to import them from others who have already created the report you want. This technique allows administrators to share reports quickly and easily. Here is a list of some popular sites where you can download examples:

`http://blog.coretech.dk/category/confmgr/config-mgr-inventory-and-reporting/` Contains ready-made reports to download and import. Offers step-by-step descriptions of how to create and modify reports.

`http://myitforum.com/cs2/blogs/sthompson/default.aspx` Personal blog of Steve Thompson, long-time Configuration Manager and SQL MVP. Steve publishes full reports as well as useful troubleshooting tips.

`http://www.myitforum.com` Large online System Center community where you will find several community leaders and contributors posting reporting solutions.

Please see the Microsoft Technet Library article detailing how to create custom reports by using SQL Server Views in System Center 2012 Configuration Manager at `http://technet.microsoft.com/en-us/library/dn581954.aspx`.

Note that there are many other community websites that contribute with the SQL reporting knowledge base and the previous list provides just a base reference.

Importing Reports

Unlike in previous versions of Configuration Manager, you will not be able to import reports using the Configuration Manager console. Instead you will use Report Manager and upload an RDL file as described here:

1. Open a browser and connect to `http://reportingserver/reports`.
2. Open the `ConfigMgr_<SITECODE>` folder.
3. Click New Folder, and enter a name like **`Mastering Configuration Manager 2012`**. Click OK when finished.

4. Open the newly created folder and click Upload File.
5. Click Browse, select the report file, and click Open.
6. You can type a new name for the report; click OK when finished.

   It is very likely that the data source specified in the report is not valid and needs to be changed after the import.
7. Hover the mouse over the right side of the report to access the drop-down arrow, and select Manage.
8. Select Data Sources.
9. Select A Shared Data Source and click Browse.
10. Navigate to the Configuration Manager site folder, and select the data source.
11. Click OK.
12. Back in Data Sources, click Apply.

The newly imported report is now ready for use and will also be imported into the Configuration Manager administrative console.

Exporting Reports

Exporting reports also requires that you use Report Manager and download the report as described here:

1. Open a browser and connect to `http://reportingserver/reports`.
2. Open the `Configuration Manager 2012` folder.
3. Navigate to the report you want to export.
4. Open the report properties as explained previously in this chapter.
5. Select Properties and click Download.
6. Click Save, and save the RDL file to a location of your choice.

The Bottom Line

Install the Reporting Services point. Installing a Reporting Services site system within Configuration Manager allows not only administrators but everyone to view reports in some fashion either via different file formats or a direct link within the Report Manager Website.

Master It What is the procedure to enable Reporting with Configuration Manager?

Manage reporting security. Reporting security is an integrated part of the built-in security. You provide users with access to reports by adding them to a predefined security role or by creating a custom role with permissions to run or modify reports.

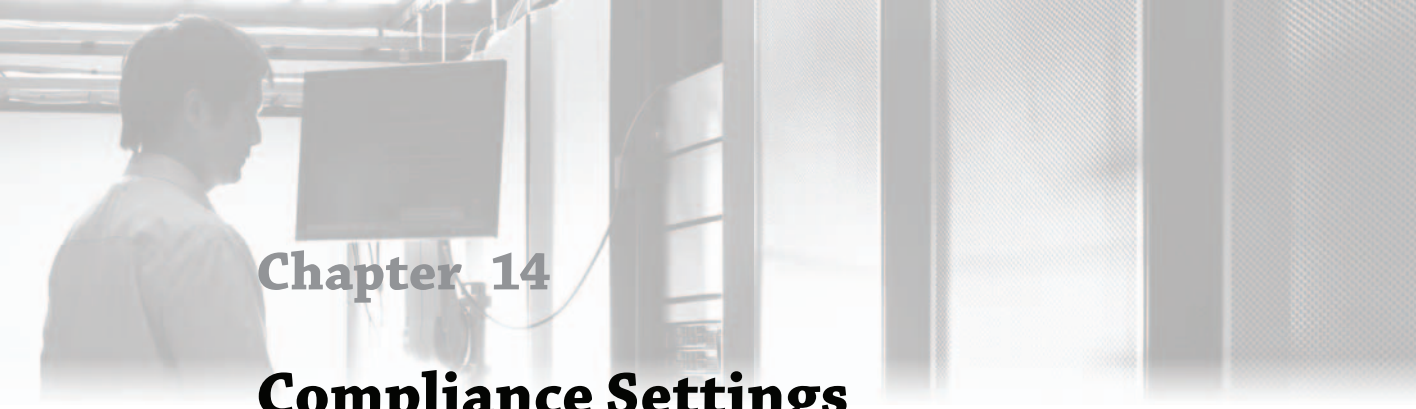
Master It Add users to a built-in security role.

Create and manage report subscriptions. Creating subscriptions can be very helpful in many scenarios. You can configure subscriptions from Report Manager or in the Configuration Manager console.

Master It Create an email-based subscription.

Create custom reports. Creating custom reports can be helpful in many scenarios. You will quickly find that the canned reports are very useful but may be limited for all your needs.

Master It Create a custom report.



Chapter 14

Compliance Settings

The Compliance Settings feature in System Center 2012 R2 Configuration Manager allows you to assess the compliance of client devices with regard to a number of configurations, such as whether the correct operating system version is installed and configured appropriately, whether all required applications are installed and configured correctly, whether optional applications are configured appropriately, and whether prohibited applications are installed on your clients. Additionally, you can check for compliance with software updates, security settings, and mobile devices. Configuration item settings for the Windows Management Instrumentation (WMI), the registry, and scripts in ConfigMgr 2012 allow you to automatically remediate noncompliant settings when they are found.

Compliance Settings is the new name for ConfigMgr 2007 *Desired Configuration Management* (DCM). With the new name come changes to the UI by simplifying the process of creating compliance settings, which ensures that IT professionals can remediate those noncompliant settings.

In this chapter, you will learn to

- Enable the client settings
- Create configuration items
- Define a configuration baseline

Overview of Compliance Settings

Compliance settings are evaluated by defining a configuration baseline that contains the configuration items you want to monitor and rules that define the required compliance. This configuration data can be imported from `http://pinpoint.microsoft.com` in Microsoft System Center Configuration Manager configuration packs, defined as best practices by Microsoft and other vendors, defined within Configuration Manager, or defined externally and then imported into Configuration Manager.

After a configuration baseline is defined, it can be deployed to devices through collections and evaluated on a schedule. Client devices can have multiple configuration baselines assigned to them, which provide the administrator with a high level of control.

Client devices evaluate their compliance against each configuration baseline they are assigned and immediately report back the results to the site using state messages and status messages. If a client is not currently connected to the network but has downloaded the configuration items referenced in its assigned configuration baselines, the compliance information will be sent on reconnection.

You can monitor the results of the configuration baseline evaluation compliance from the Deployments node of the Monitoring workspace in the Configuration Manager console. You can also run a number of compliance settings reports to drill down into details, such as which devices are compliant or noncompliant and which element of the configuration baseline is causing a computer to be noncompliant. You can also view compliance evaluation results from Windows clients on the Configurations tab of Configuration Manager in the Windows Control Panel.

What's New in Configuration Manager 2012 R2?

The following Compliance Settings features are new or have been changed since Configuration Manager 2007 (see Figure 14.1).

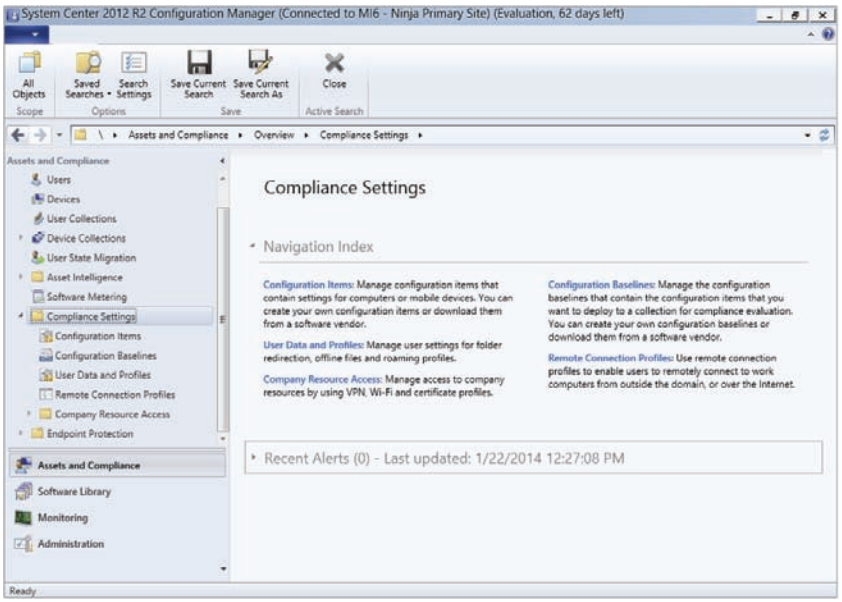


FIGURE 14.1 Compliance Settings main page

- Configuration Manager 2007 Desired Configuration Management is now called Compliance Settings in Configuration Manager 2012.
- The process of creating configuration baselines has been simplified.
- Settings can be reused for multiple configuration items.
- Remediation is supported for WMI, registry, and script settings that are noncompliant.
- Configuration baselines can be deployed to users and devices.
- Compliance Settings can be used to manage mobile devices in the enterprise.
- You can create user data and profiles configuration items that contain settings that control how users in your hierarchy manage folder redirection, offline files, and roaming profiles on computers that run Windows 8.
- The new Mac OS X configuration item lets you evaluate and remediate preference (`.plist`) settings on Mac computers. You can also use shell scripts to evaluate and remediate other Mac settings.

- New mobile device settings and mobile device setting groups have been added.
- Remote connection profiles, company resource access, certificate profiles, VPN Profiles, and Wi-Fi profiles can be created in this new section.

What Can You Do with Compliance Settings?

The best answer is that with Compliance Settings you can automatically check the compliance of your Configuration Manager clients against standards that you choose. Those standards can be company policies regarding how a computer is configured, policies for compliance with regulations such as Sarbanes-Oxley (SOX), or best practices defined by a vendor or based on your internal IT department's experience. For example, they can be settings that a department manager has decided all the computers within the department must meet or a means to identify computers that need more memory as defined by the IT manager in charge of desktops.

Given that range of potential applications, the next question is, what settings can you check with Compliance Settings? This seems like an easy question to answer, but of course it isn't. So, let's explore what you can and cannot do with Compliance Settings.

Let's examine this from a different perspective, and then it will be clear what exactly you can and cannot check for using Compliance Settings.

Configuration Items

Configuration items (CIs) are the smallest single settings or standards that you assemble with other CIs to create a configuration baseline, which is then applied to Configuration Manager clients. You can choose from specific types of configuration items to create these checks:

- Application CIs
- Operating system CIs
- Software update CIs
- Mobile device CIs
- Mac OS X CIs
- General CIs

These checks are keys to understanding the limits of what you can do with Compliance Settings. When you choose the type of configuration items using the wizard in the Configuration Manager console, it will determine what types of checks you are allowed to include as part of a CI. Table 14.1 summarizes the main CI types.

Table 14.1: Configuration item types

Type	Definition	Example
Application	Used to check an application's settings for compliance	Checking Microsoft Office Word for the latest `Normal.dot` file
Operating system	Used to check a particular operating system's version or settings for compliance	Checking to ensure that Configuration Manager clients have the latest service pack for Microsoft Windows Vista installed

TABLE 14.1: Configuration item types *(CONTINUED)*

Type	Definition	Example
Application	General, Objects, Settings, Detection Method, Applicable, Security	Windows Version
Operating system	Windows Version, Objects, Settings, Security	Detection Method, Applicable
Software update	General, Security	Windows Version, Objects, Settings, Detection Method, Applicable
General	General, Objects, Settings, Applicable, Security	Windows Version, Detection Method

As you would expect, not all of these configuration item types offer the same properties. For example, the operating system type contains a property to check for the exact build of the operating system that is running on the Configuration Manager client being evaluated; this option is not available in the other configuration types. As mentioned earlier, a configuration baseline can (and almost always will) contain multiple configuration items of all configuration types. The properties available to each configuration item type are listed in Table 14.2.

TABLE 14.2: Properties of configuration item types

Type	Available	Not Available
Software update	Used to check Configuration Manager clients for software update compliance	Checking the status of approved software updates on Configuration Manager clients
Mobile device	Used to check and enforce settings on supported mobile devices	Checking to ensure an unlock PIN setting is enforced to secure the device
Mac OS X	Used to check settings for compliance on supported Mac OS X devices	Checking a preference list to ensure corporate settings are configured
General	Used to check settings of objects that do not fall under the other categories	Checking the hosts file to ensure that spyware has not modified the file or that the system has the latest hosts file installed

The reason for restricting configuration item types to specific properties, instead of having a single type with all properties available, is to keep the configuration items as small as possible. Defining configuration items as specific types allows you to reuse them when you create configuration baselines. For example, you can create an operating system configuration item that checks for Microsoft Windows 8.

Additional objects and settings are available when you create this configuration item type. You can also check for the presence of a specific file and its attributes. You can run validation against an assembly that is present, and you can even check the string value of a registry key and report on noncompliance for any of these objects or settings, all within the same configuration item. But if you design your configuration items with the idea of being able to reuse them in multiple configuration baselines, they should be as lean and specific as possible. If you need the configuration item to validate something else for a particular scenario, you can simply create a child configuration item. This configuration item will inherit all the original settings of the configuration item and allow you to add additional validations, leaving the original configuration item intact and not affecting any of the configuration baselines that are using that configuration item.

Configuring Compliance Settings Client Settings

Configuring the Compliance Settings client settings is as easy as selecting Yes or No for the Enable Compliance Evaluation On Clients option and determining the appropriate schedule for clients to evaluate their compliance. This setting is located in the Administration workspace under Overview ➢ Client Settings ➢ Default Client Agent Settings. Then right-click and select Properties. This will open the properties window for the client settings (see Figure 14.2). By setting the Enable Compliance Evaluation On Clients option to Yes, you enable this option in the default settings. The default schedule for evaluation is every seven days. You can adjust this schedule as necessary for your environment, including using a custom schedule that will allow you more control over when it runs, but the default schedule will typically be adequate for most environments. You can also modify the default client settings, create new custom client settings, or modify existing custom client settings. You can create or modify custom client settings when you want to apply a group of client settings to specific collections.

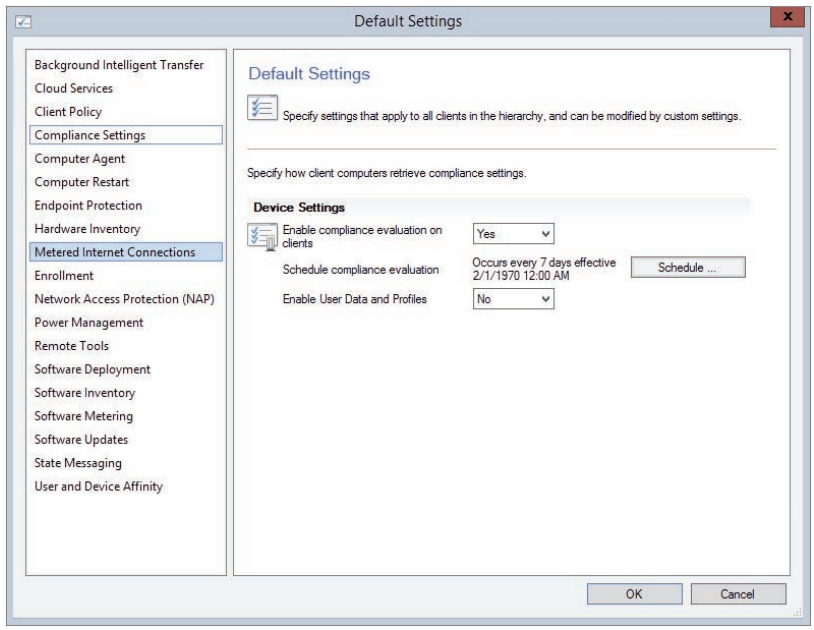


Figure 14.2 The default client settings

Creating Configuration Items

Configuration items are pieces of the configuration baseline that, when assembled, will allow you to monitor configuration drift from what you have specified. To demonstrate the processes of creating configuration items and a configuration baseline, we'll use a utility called Microsoft Calculator Plus, described in the accompanying sidebar. Because there are so many ways to configure this product and use it, we'll demonstrate its use throughout this chapter so you can gain a better understanding of Compliance Settings. You can then take these examples and apply them to any product you choose.

Calculator Plus

This application is a mathematical calculator that allows you to complete many different types of conversions; it also includes all the mathematical functions offered in Microsoft Calculator. This is a very small application, which is why we selected it to use in this example.

To download this application, go to

```
http://www.microsoft.com/download/details.aspx?id=21622
```

You will need to install this application on your ConfigMgr client.

Start by opening the Configuration Manager console, if necessary. From the Assets And Compliance workspace, expand Overview; then expand Compliance Settings, right-click Configuration Items, and click Create Configuration Item. You should be on the General page of the Create Configuration Item Wizard, as shown in Figure 14.3.

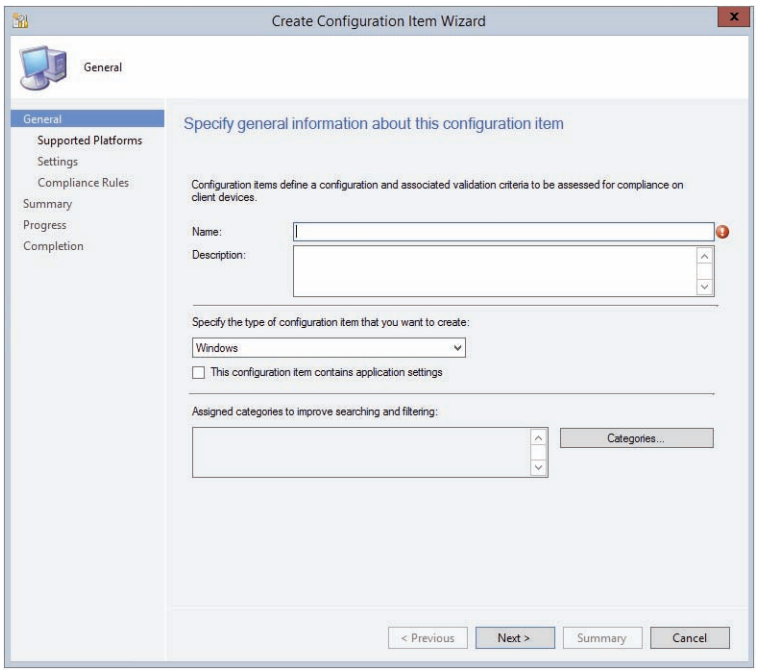


Figure 14.3 The Create Configuration Item Wizard - General page

To create a new configuration item, follow the instructions in the wizard. As part of this chapter you will be guided through the steps to create your first configuration item and apply this to any collection for evaluation. In this example we will validate that Microsoft Calculator Plus is installed. You could also use any of the applications discussed in Chapter 8, "Application Deployment."

Name, Description, and Category

In the Create Configuration Item Wizard, you begin on the General tab. Fill in the Name and Description fields and then create a category before moving to the next tab:

1. In the Name field, type **Microsoft Calculator Plus - Installed**.
2. In the Description field, type **This configuration item validates that the Microsoft Calculator is installed.**
3. Then, still in the Description field, press Ctrl+Enter to simulate a carriage return and add something descriptive stating when and by whom this item was created or changed.

   You could use your initials or the current date or a combination; it just needs to be something that will help you later know who created or changed the item and when, so that if anyone has a question about your configuration item, they know who to contact.
4. Click the Categories button to open the categories list.

   The list is populated with a few default categories, and the top section allows you to add your own custom categories.



Real World Scenario

What Is a Good Category?

This will depend on your own administration style to a certain degree as well as the number of configuration items you will be creating. If you plan to check only Exchange servers for configuration drift, then you may not need any additional categories or just a few more. If you plan to check clients for application settings, Internet Explorer for configuration drift, different operating systems files for the correct security settings, and so on, you would probably be wise to set up a standard for determining when new category types are needed and when you can use existing ones.

We have seen administrators who set up categories for every possible difference and others who set up none. If you are going to use the categories and build a large number of configuration items and baselines, then you should set up custom categories, but don't go overboard. Remember that categories are used to sort and search, so if you have too many, you get little or no benefit; too few is the same as none. It's best to use simple rules to create a standard: Does this configuration item fit into a category that exists already? Does that category generally and easily define this configuration item's purpose? If the answer is no to either, then you probably need a new category.

For this example we are going to create a new category.

5. In the Add A New Category section, type **Microsoft** and click the Add button.

   This should add it to the Administrative Categories section and select it.
6. Before you click OK, verify that your categories look like those in Figure 14.4.

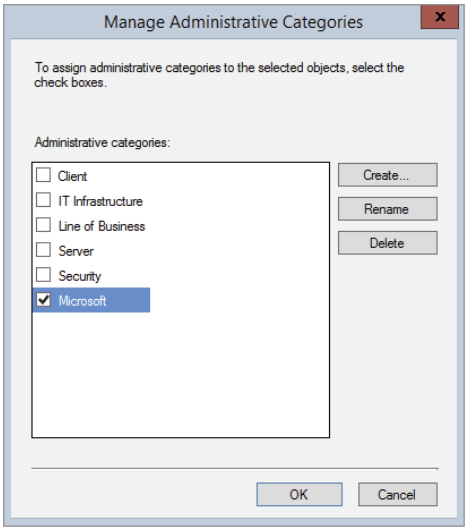


FIGURE 14.4
The Create Configuration Item Wizard's Manage Administrative Categories dialog box

7. Click OK to return to the General tab in the Create Configuration Item Wizard, which should now contain the item's name, a description, and your newly created category.
8. Verify that your dialog looks the same as Figure 14.5, and then click Next.

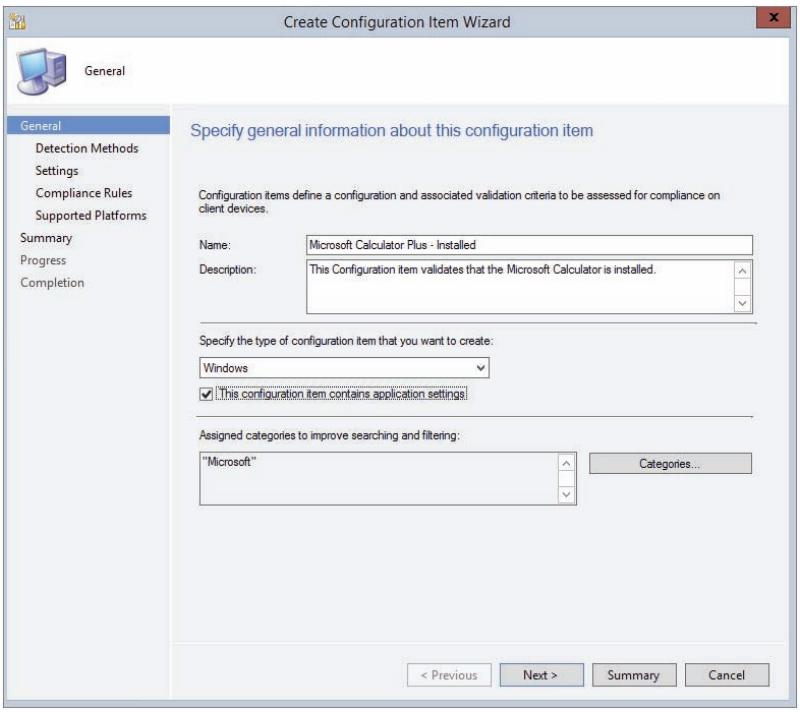


FIGURE 14.5
Create Configuration Item Wizard - General page completed

Choosing a Detection Method

The next tab in the wizard is Detection Methods, which is unique to the application configuration item type; it is not offered with the other types. The purpose of this tab is to specify the method used to verify that the application being checked for is installed on the client.

Four options are available:

- The first is Always Assume Application Is Installed.

  This will skip any verification check, which sounds great; you're essentially telling the system to check the application for just the settings you're about to specify. But if you do this while using certain rules in creating your configuration baseline, you will run into problems.

Baseline Rules

Which baseline rules cause problems? You will need to decide which if any of the following are problematic:

- If these optional application configuration items are detected, they must be properly configured.
- These application configuration items must not be present.

If another baseline is dependent on these configuration items, it may invalidate your dependency.

- The second option, Use Windows Installer Detection, is used to verify the product code the application vendor included with the MSI installer and the version.
- The third option is Detect A Specific Application And Deployment Type; you can select an existing application and deployment type that has been previously created.
- The final option is Use A Custom Script To Detect This Application; you can use VBScript, JScript, or PowerShell.

In the following procedure, you'll use the second option:

1. Select the Use Windows Installer Detection radio button.

   This will require you to have access to the installation files, but if you downloaded the Microsoft Calculator Plus application from the Microsoft Downloads site, you should already have this file. If not, please download it now.

2. Assuming you have the Microsoft Calculator Plus files downloaded and extracted, click the Open button on the Detection Methods page, and browse to the folder where you saved the MSI file.

3. Find and double-click the `calcplus.msi` file, and it will populate the Product Code and Version fields on the Detection Methods page.

   If this application is installed on a per-user basis, you may also need to check the corresponding box for it to be properly detected. If it was installed for all users, that is not necessary.

4. Before moving on to the next step, creating and validating an object, verify that your wizard settings look similar to those in Figure 14.6. (Your product code and version number may be different.)

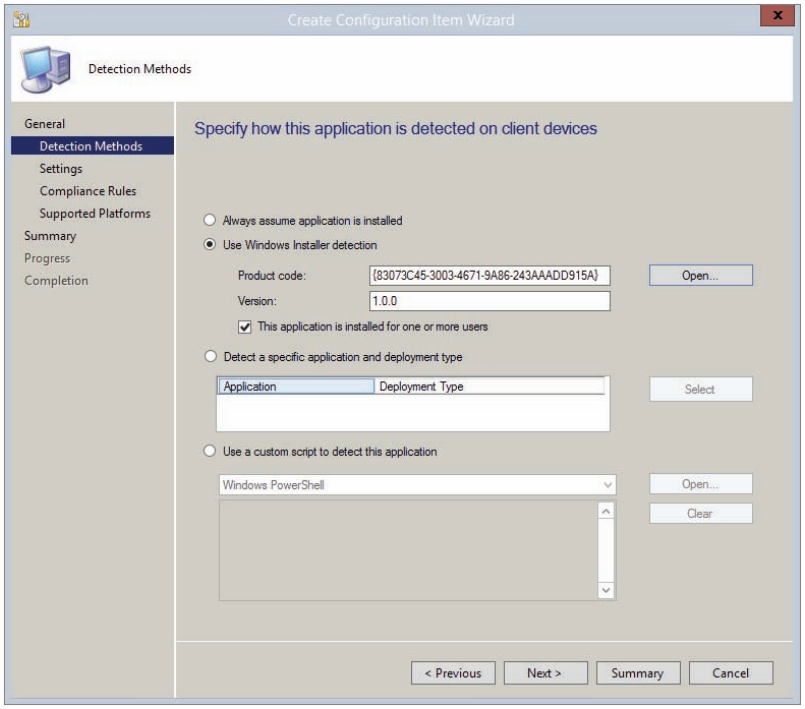


FIGURE 14.6
CI application Detection Methods page

5. If everything is in order, click Next to proceed to the Settings tab.

Creating and Validating a Setting

On the Settings page, you tell the Create Configuration Item Wizard what type of setting to look for and where that setting is found.

CREATING A SETTING

In the empty window there are four columns—Name, Setting Type, Inherited, and User Setting—and a New button.

1. Click New (see Figure 14.7); a Create Setting window will appear, as shown in Figure 14.8.

   The General tab of the Create Setting window has several fields and drop-down menus. The red circles with exclamation points indicate that the blank fields require input before you can create the configuration item.

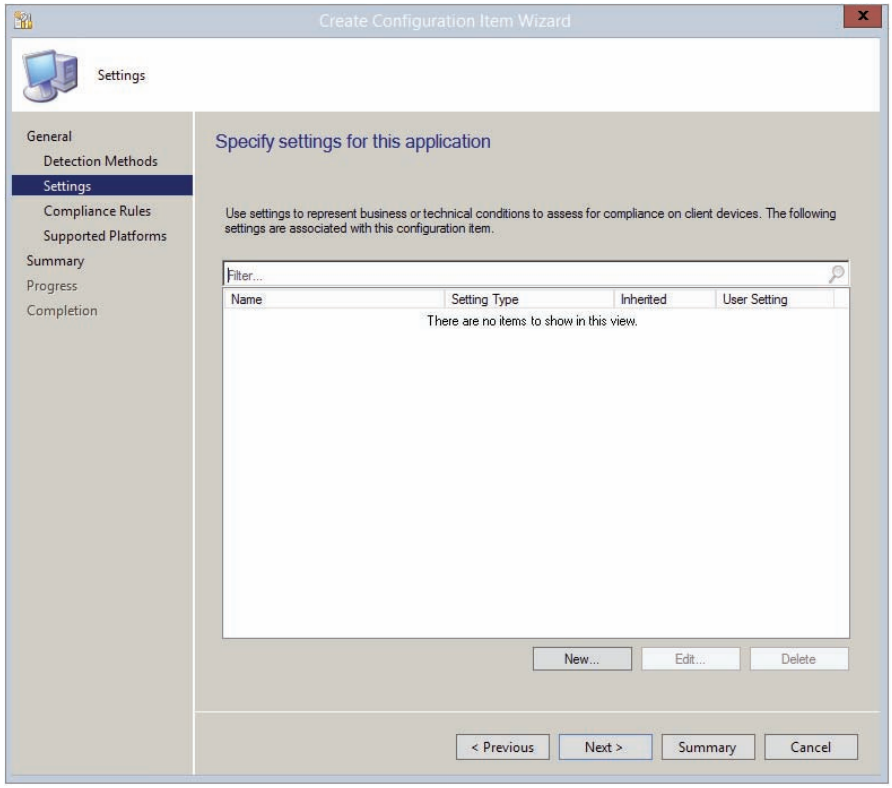


FIGURE 14.7
CI application Settings page

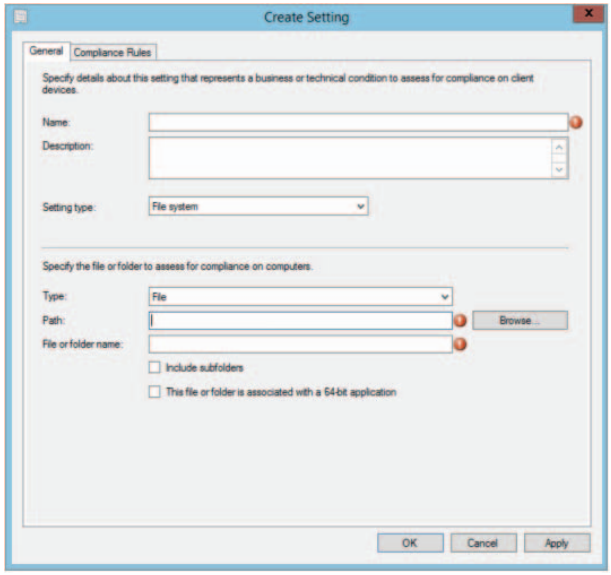


FIGURE 14.8
Create Setting dialog box

2. From the Setting Type drop-down menu, select File System.
3. In the Path field, enter **C:\Program Files (x86)\Microsoft Calculator Plus**, and in the File Or Folder Name field, enter **calcplus.exe**.

Wildcards and Environment Variables with Compliance Settings

The use of wildcards is allowed and actually required for the Specify File Or Folder To Assess For Compliance On The Computer section in the Path field. The ? and * characters are the permitted wildcards, but you should carefully consider whether to use them. Using wildcards can produce additional overhead when you're trying to find a file or folder, because the search will work exactly as instructed. Specifying the Windows directory, for example, and then telling it to search all sub-directories is not ideal. You can also make use of environment variables such as `%ProgramFiles%` or `%AllUsersProfile%`. The result may be that you get more than one result if the users all have the file or folder you are looking for in the search path.

4. In the Description field, enter **This configuration item locates the file calcplus.exe and validates that it is the latest version of this file**.
5. You can leave the This File Or Folder Is Associated With A 64-Bit Application check box unchecked for Microsoft Calculator Plus.

64-Bit Applications and the Registry

Readers who have 64-bit applications should be aware of a possible issue with the registry and configuration baselines. Because of the registry reflector that mirrors certain registry keys for interpretability, it is possible that you could detect the presence of two registry keys with a single configuration baseline. If you are running 64-bit applications, you will need to check for this before deploying a configuration baseline containing a configuration item that involves checking for a registry key associated with a 64-bit application.

You have finished creating the object's details by telling Compliance Settings what you are looking for and where to look for it. The next step is to validate the setting by telling Compliance Settings the specifics of the setting to validate.

6. Before you click OK to move to the Compliance Rules tab, make sure your General page looks like the one in Figure 14.9. Click Next when ready.

Validating a Setting

Now that you have created your setting, you need to tell Compliance Settings how you want this CI to validate the file.

1. As you did when creating a new setting, click the New button, shown in Figure 14.10, to get started.

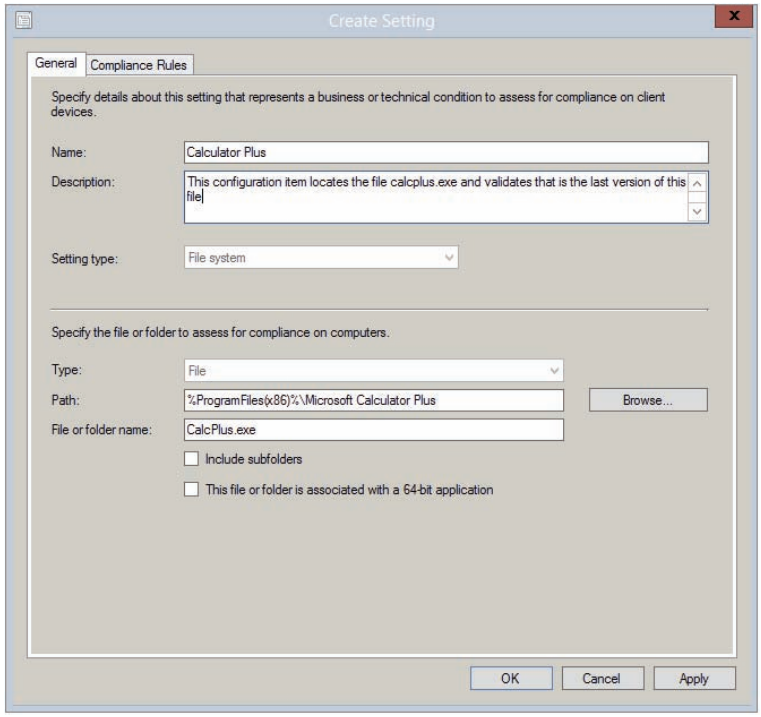


FIGURE 14.9
General page of the Create Setting dialog box completed

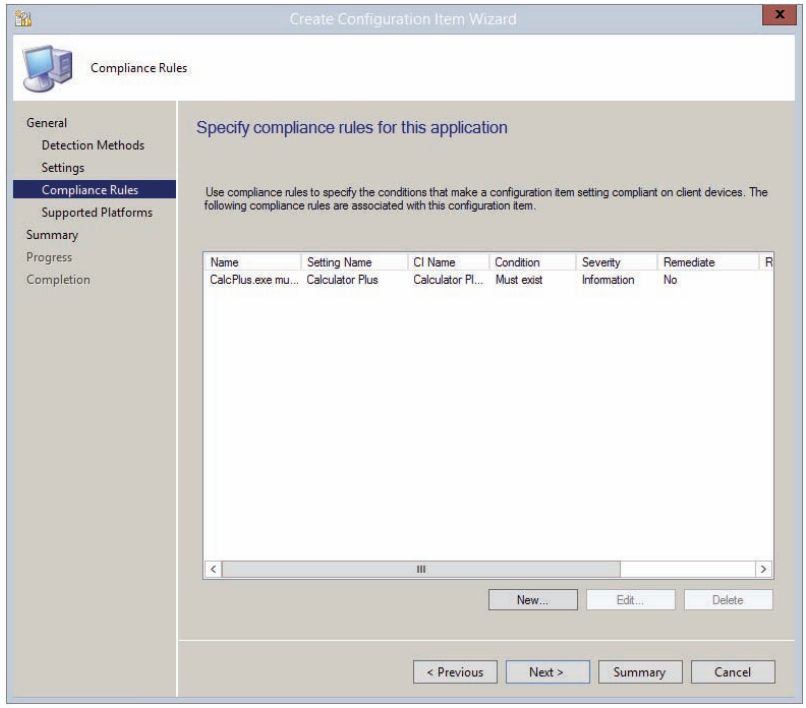


FIGURE 14.10
The Compliance Rules page

The top field of the Create Rule dialog box contains the name of the compliance rule. This is a required field, and a value will be supplied by default.

2. In the Name field, enter in a rule name of **File_calcplus.exe_Date Modified**.
3. Click Browse.
4. Select Microsoft Calculator Plus - Installed, the CI name that you previously created. Click Select.
5. In the Description text box, enter the following or something similar, but make sure you also put your initials and the date in the event someone else reviewing this rule has questions: **Validates that the calcplus.exe file in the Microsoft Calculator Plus folder has the latest version of the file approved and distributed by IT. 12/13/2013**

   In the Create Rule dialog box, you tell Compliance Settings exactly how to validate this file. The Setting Must Comply With The Following Rule field in the middle of the page is grayed out and unavailable because you have already selected the type of setting you are going to validate against. Next to that is a drop-down menu, where you have nine operators to choose from:

   - Equals
   - Not Equal To
   - Greater Than
   - Less Than
   - Between
   - Greater Than Or Equal To
   - Less Than Or Equal To
   - One Of
   - None Of

   If you choose Between as the operator, you get the option to specify a range.
6. In this example, choose the Equals operator, and in The Following Values field, enter the date and time for which you want the rule to be applied.

   Obviously, because you are going to use this as a test, you should make a change to the file so that the modified date is not its original date, or input your validation date and time.

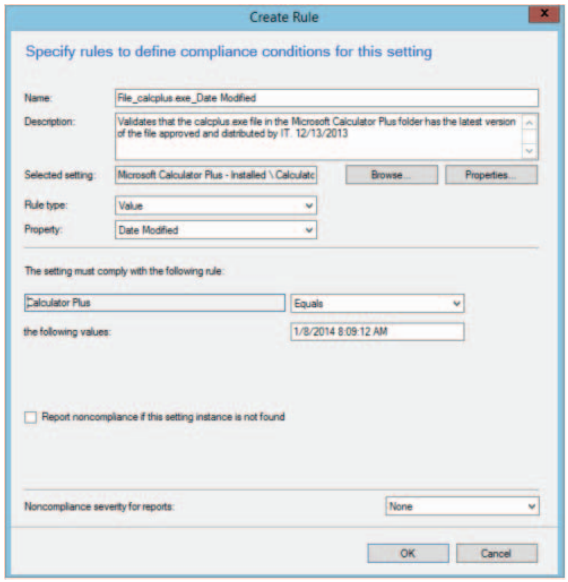
   In the bottom section of the Create Rule dialog, choose the level of Noncompliance Severity For Reports should this check fail on one of your Configuration Manager clients. There are five levels to choose from:

   - None
   - Information
   - Warning
   - Critical
   - Critical With Event

The Information, Warning, Critical, and Critical With Event levels report back to Configuration Manager, but the None does not write an event to the application event log in Windows as the last one does. This was made an option to prevent Compliance Settings rules from filling up the event logs on clients if a check comes back as invalid too many times. This might happen if, for example, you input the wrong validation data or if something out of your control occurs, such as an upgrade or service pack installation.

7. In this exercise, select None if you don't already have it selected, and then verify that your window looks like Figure 14.11 before clicking OK to continue.

FIGURE 14.11
The Compliance Rules - Create Rule dialog box



8. Return to the Compliance Rules window, where in the formerly empty section you'll now see the new compliance rules for this file.

   You now have to tell Compliance Settings if you want it to report on a noncompliant event and, if so, the details of when and how it should report.

   Select the File_calcplus.exe_Date Modified rule you just created, and click Edit. Check the Report Noncompliance If This Setting Instance Is Not Found check box so that it is enabled.

   This option turns on and off the reporting of a noncompliant client and allows you to set the severity of noncompliance as well as at what point it should report. Click OK.

9. You have now created your first compliance item. After reviewing all information and verifying that it is correct, click Next to validate the supported operating systems.

   This is the only object you are going to create in this first example, but we'll cover other tabs and their options in the following examples or in later examples.

10. Because you are not going to make changes to this configuration item, you can click through to the end using the Next button at the bottom of the window.

    Eventually you should reach the Summary tab, shown in Figure 14.12, which will give you a list of all the options and settings selected while creating this configuration item.

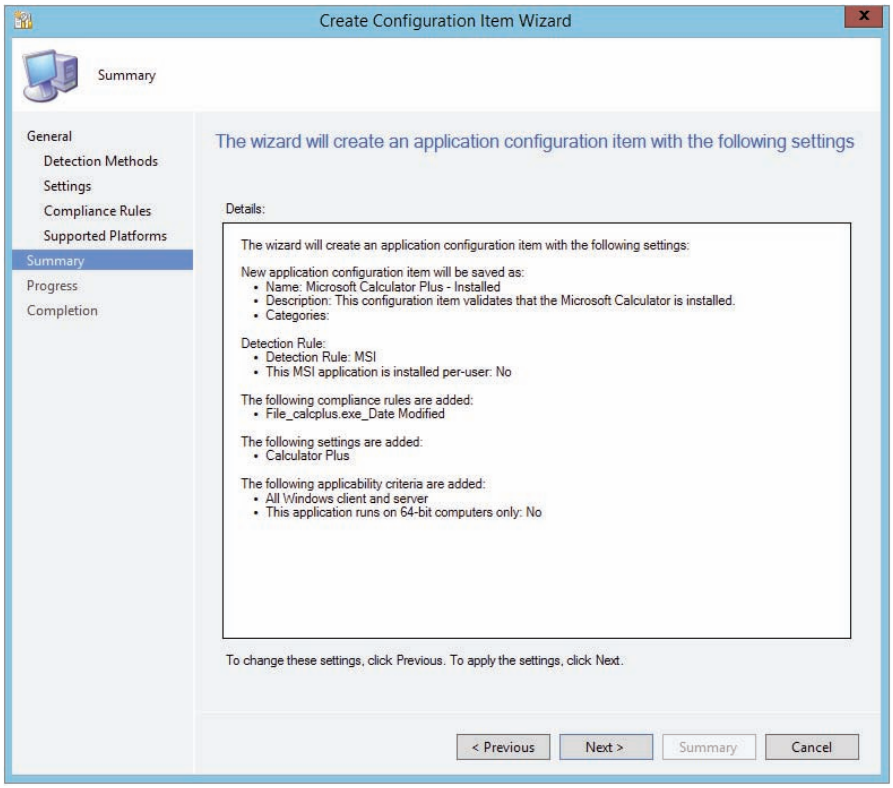


FIGURE 14.12 Application CI Summary page

11. Verify that the settings are as you expect them to be; if any are not, use the Previous button or the tabs to make any modifications.

12. Once you have checked to ensure that everything is in order, click the Next button or the Progress tab to start the process of building the configuration item.

    After a short period, the progress indicator and window should disappear and you should see the Completion window, which says

    ```
    Success: The Create Configuration Item Wizard completed successfully.
    ```

    It also shows a list of the settings you chose. Verify again that everything is listed as expected. You can now click the Close button to complete the wizard and return to the Configuration Manager console.

Building a Configuration Baseline

You have built a configuration item to make your configuration baseline, which is what you assign to your clients to check for drift.

Briefly, you have a configuration item that validates that your Microsoft Calculator Plus application is installed and the file is the latest file you deployed. In order to deploy this compliance setting and rule, you need to create a baseline and apply this baseline to a specific collection to validate its compliance.

Configuration baselines in System Center 2012 R2 Configuration Manager contain predefined configuration items and optionally other configuration baselines. After a configuration baseline is created, you can deploy it to a collection so that devices in that collection will download the configuration baseline and assess their compliance with it.

Configuration baselines in System Center 2012 R2 Configuration Manager can contain specific revisions of configuration items or can be configured to always use the latest version of a configuration item.

Creating the Initial Baseline

As it does with most tasks, Configuration Manager provides a wizard to guide you in creating a configuration baseline.

1. In the ConfigMgr 2012 console choose the Assets And Compliance workspace, select Overview ➢ Compliance Settings ➢ Configuration Baselines, and right-click Create Configuration Baseline.

   You should now see the Create Configuration Baseline Wizard, shown in Figure 14.13. Here you select the categories and input the name, description, and configuration data.

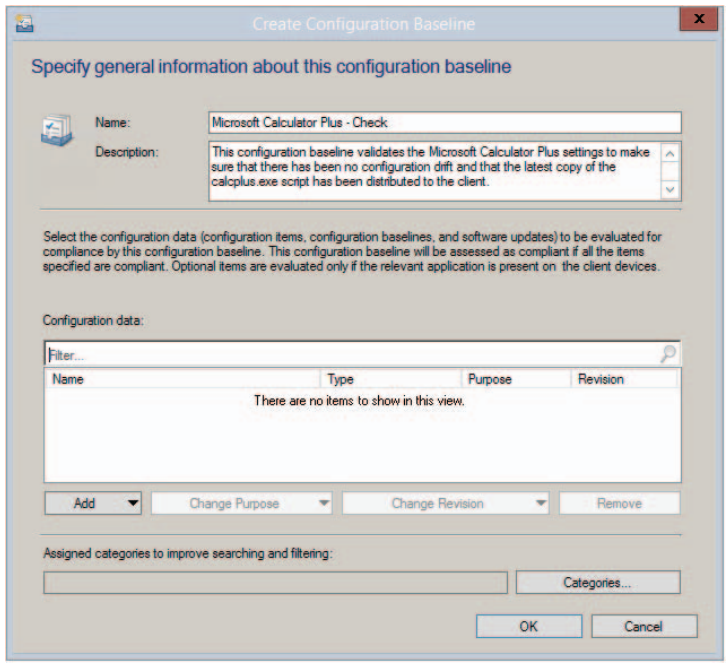


FIGURE 14.13
Create Configuration Baseline Wizard - Create Configuration Baseline dialog

2. Fill in the following details:

   Name: **Microsoft Calculator Plus - Check**

   Description: **This configuration baseline validates the Microsoft Calculator Plus settings to make sure that there has been no configuration drift and that the latest copy of the calcplus.exe script has been distributed to the client.**

3. To select Microsoft as the category, click the Categories button to display a list. This section is at the bottom of the window.

   The Configuration Data list displays all the configuration items or configuration baselines that are included in the configuration baseline.

4. Click Add to add a new configuration item or configuration baseline to the list. You can choose from the following:

   Configuration items

   Software updates

   Configuration baselines

5. Once the Add Configuration Items window checks for available configuration items, choose Microsoft Calculator Plus - Check.

6. Click Add, and then click OK.

7. Verify that your settings match those shown in Figure 14.13 and click OK.

You can now click the Close button and return to the Configuration Manager console, where you will next assign your new configuration baseline to clients that will be evaluated for compliance.

Baseline Rules

The process of creating rules is similar to the way you build rules in Outlook. Or you can think of it as telling Compliance Settings a story or writing a recipe to build your baseline. The available rules include those that reference which operating system you want to check for; in this option you will be able to see all the different operating systems and service pack levels. If you have not built a configuration item to check for a specific operating system, when you click the link in the rule there will be no configuration items to choose from and nothing to put into this rule. Although our example doesn't include them, Figure 14.14 illustrates the additional selections available when you have created one or more CIs.

One available rule is Checking For Software Updates. Earlier in the chapter we mentioned that you cannot create CIs for software updates in the same location as the other CI types and you must specify the updates when creating your configuration baseline; this is exactly where you would specify the software updates to check for. If you click the link in the software update rule, this option will show up on step 4 of "Creating the Initial Baseline." It will spawn a new window called Add Software Updates (see Figure 14.15), where you will see the same folder display as in the Configuration Manager console, and you will have all the updates that you set to download to your server available to choose from. It is important to understand that you will not see software updates that you have already added to the baseline. You can see the software updates that are included in the configuration baseline by viewing its properties in the Configuration Manager console.

FIGURE 14.14
Add Configuration Items

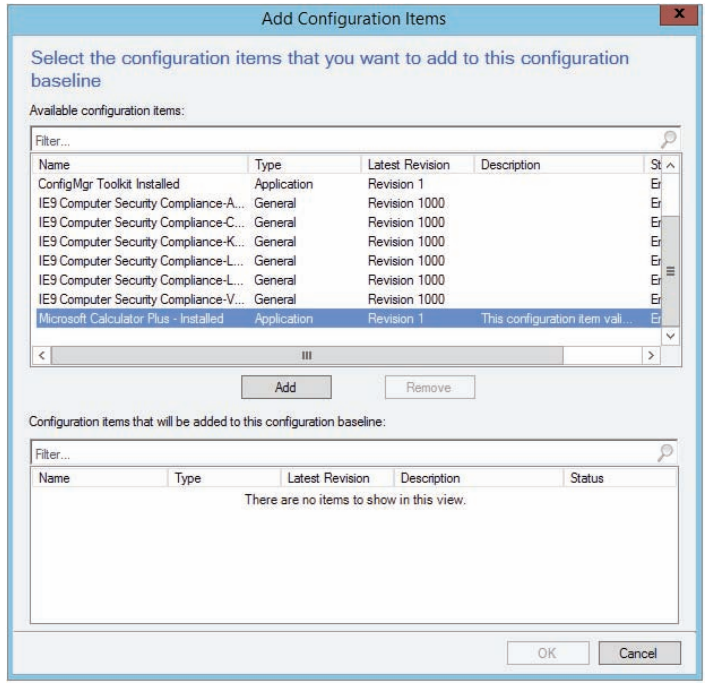
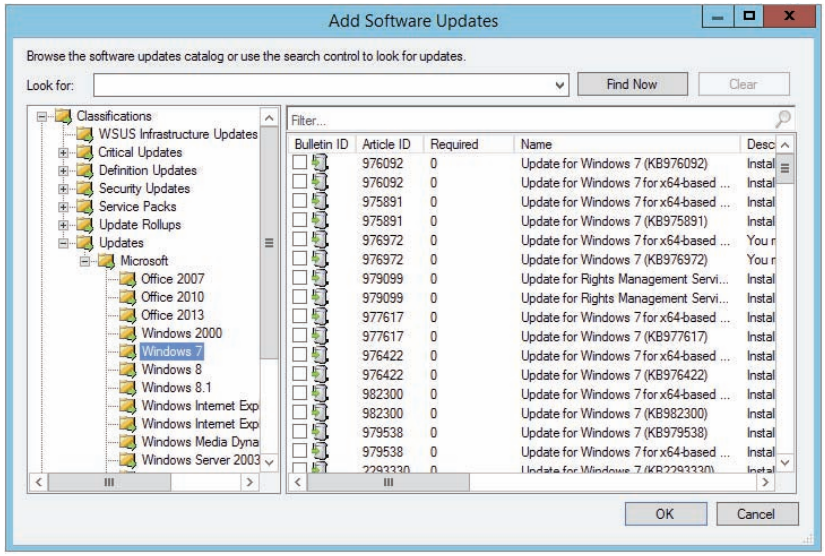


FIGURE 14.15
Add Software Updates window



Another rule that you can build is Configuration Baselines. This is how you would reuse other configuration baselines that you have created and thus save quite a few steps. Clicking this rule opens another window that lists the configuration baselines previously created and available to select, much like Figure 14.14.

We have saved the other three rules for last because they are all related to application CI types, differing in the way that they build the rules for your baseline. An application-type CI can be marked in one of three ways:

- Required
- Optional
- Prohibited

Let's consider how each of these might be used when building a configuration baseline.

Required

This rule means that if you select an application CI, it will use the detection method specified to ensure that the application is installed. We used two different detection methods when we built the application CIs for Microsoft Calculator Plus. For the first one, we pointed it at the MSI file and got the version and GUID.

When you build an application CI and use the "always assume installed" detection method, you are simply skipping the detection method. Thus, there is no chance that the detection method will fail, and the next step in your application CI will do its check. Once a CI fails a check, the remainder of the CI checks to see if settings or objects are not validated against the client. The actual status returned can vary depending on these settings as well; if the detection method is specified and it fails, it will return Not Detected compliance.

You would use this to add general CIs to your list of rules but also for applications that you want to ensure are installed, or at least to detect that they are installed and that they are configured correctly. Going back to the CIs we created for Microsoft Calculator Plus, if we specified the CIs that detect if the latest `calcplus.exe` file is on the client, the CI for Microsoft Calculator Plus would first have to pass the detection method we specified, so if the version or GUID returned Noncompliant, then the rest of the CI validation would be skipped and we would get a status message indicating that the application was not detected.

Optional

The rule that if optional application CIs are detected, they must be properly configured means that if you make application CIs part of the baseline and they fail to be detected, then the validation checks that are part of that CI will be skipped; if the application is detected, it will then validate the objects or settings specified in the CI and report compliance or noncompliance. A typical use for this type of rule might be a situation in which you are not sure an application is installed on the client, but in the event that it is, you want to make sure that the application is configured correctly.

Prohibited

The last application CI rule specifies that selected application CIs must *not* be present. This type of rule could be used to make sure that an application is not present on a system. For instance, if you are checking the configuration of Microsoft Calculator Plus 5.*x*, you might want to make

sure that Microsoft Calculator Plus 4.*x* was properly removed. Assuming you had a baseline that you used to check the configuration of Microsoft Calculator Plus 4.*x*, you could select one of these rules and run it to validate that the application had been previously uninstalled.

Assigning the Configuration Baseline to Clients

Now that you have all the baselines configured, you need to assign them to the clients or all your hard work will be in vain. Assigning the configuration baselines to the clients will allow Configuration Manager to monitor the clients and ensure the baselines are met.

1. Back in the Configuration Manager console, you should still see the configuration baselines. If you highlight the newly created baseline, you will see its details at the bottom of your console.
2. To assign this configuration baseline to clients for validation, right-click the baseline and choose Deploy.

   This will start the Deploy Configuration Baselines Wizard, shown in Figure 14.16.

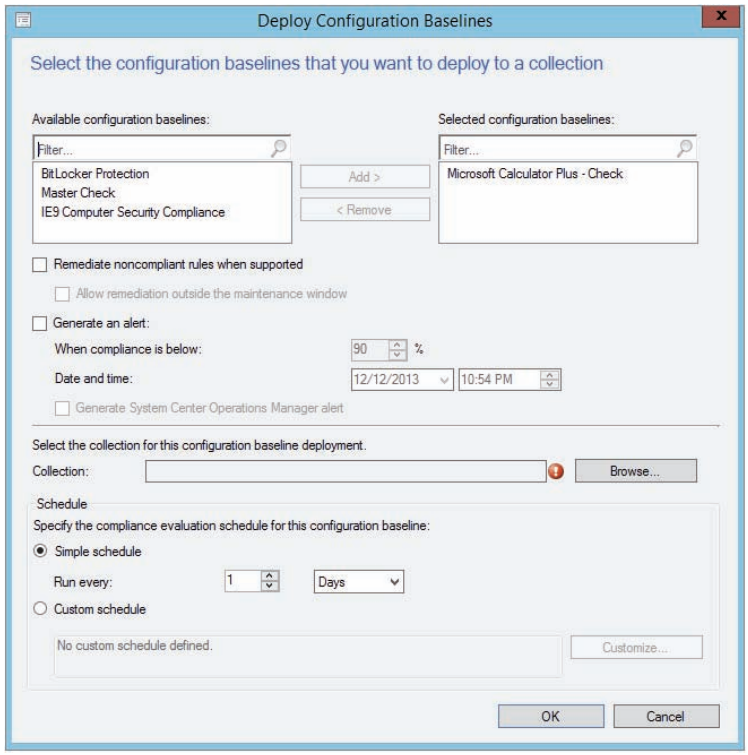


Figure 14.16
Deploy Configuration Baselines Wizard

This should prepopulate with the configuration baseline that you used to launch the wizard; as you can see, you can add or remove configuration baselines by clicking the Add or Remove button on the center.

3. At this time if you see the correct configuration baseline in the available list, select the baseline and click Add to move it to the list on the right.
4. In the Select The Collection For This Configuration Baseline Deployment section, indicate the collection you are going to assign this baseline to by clicking the Browse button.

   Be sure to select a collection that includes the clients where you have installed and configured the Microsoft Calculator Plus client.
5. After you have selected the appropriate collection, click OK to go back to the deployment baseline window.

   Next, you set the compliance evaluation schedule, much as you do with a deployment. You can create a simple schedule such as Run Every 7 Days or create a custom schedule for more flexibility.
6. For the example, choose Custom Schedule and set it to reoccur every four hours; this ensures that the validation will run and return data so you can examine the reports.
7. After reviewing the settings, proceed to assigning the baseline by clicking OK.

Additional Configuration Baseline Options

Within the Configuration Manager console, some additional options are available when you view the configuration baseline folder. On the ribbon, there is an option called Import Configuration Data. This option allows you to import a CAB file that could have been created by a vendor, using an external tool such as Silect Software's CP Studio, or it could come from another Configuration Manager site. If you have a baseline currently selected, you should see some additional options, including the ability to export configuration data. This will allow you to export your data so that you can import it to another site or edit it with an external tool.

You also have the ability to enable or disable the baseline; if you select the Disable option, it will stop the clients from evaluating this baseline. Once a baseline is disabled, the option changes to allow you to enable it from the same location on the ribbon. You can also view the XML that defines this baseline by clicking the View XML Definition button of the ribbon. The Categorize option should be self-evident at this point; you can add or remove categories from the baseline using this button.

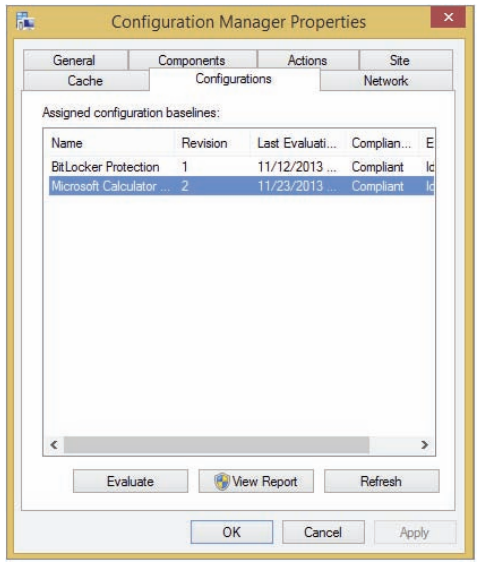
Client Validation of Compliance Baseline Rules

Once you have deployed the compliance baseline to a collection, you should log on to a client and validate that this rule has been applied and what its current state is; this will help you to understand better if the rule has been applied correctly or not and if the compliance state is the desired one.

1. Log on to the Windows client or any resource on the collection deployed.
2. Choose Control Panel ➢ All Control Panel Items, and locate Configuration Manager.
3. Open Configuration Manager and select the Configurations tab.
4. Select the Microsoft Calculator Plus baseline and click Evaluate. Note, if the client has not polled for machine policy from the Configuration Manager site server yet, you might also need to first request the machine policy update action.

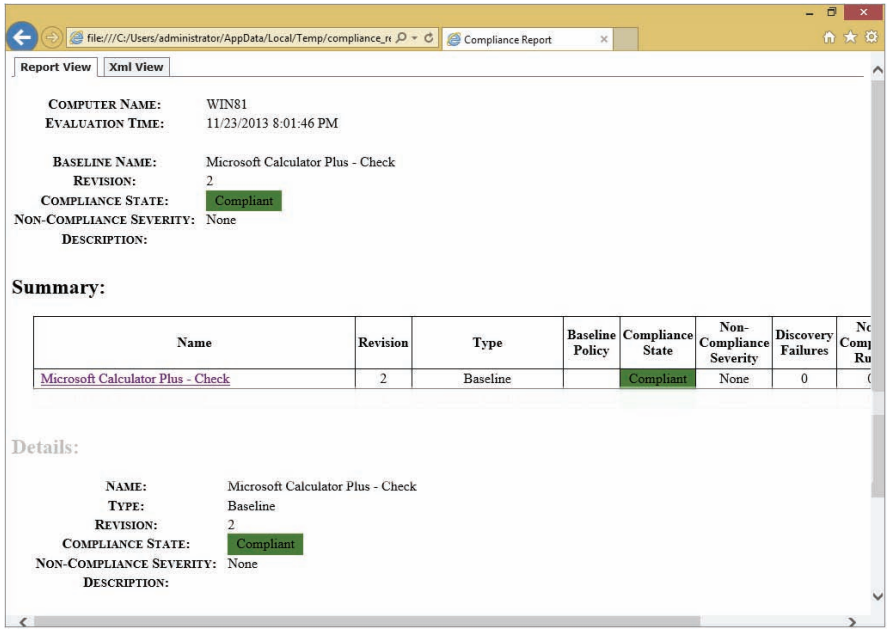
As shown in Figure 14.17, the Compliance State field now shows Compliant.

FIGURE 14.17
Configuration Manager client configurations



5. Now click View Report and wait for Internet Explorer to show the results. You can see our results in Figure 14.18.

FIGURE 14.18
Compliance Report



Once you have finished reviewing the compliance setting results, you can also look at the client log files to see more details about the compliance state; two of these log files are as follows:

dcmagent.log Provides high-level information about the evaluation of assigned configuration baselines and desired configuration management processes

ciagent.log Provides information about downloading, storing, and accessing assigned configuration baselines

Open these log files using `CMTrace.exe` and you will see more details. Now that you have been able to successfully apply a configuration baseline, you may want to try this again using a production application for which you may need to confirm its compliance state.

Compliance Settings Alerts

As part of the new alert and notification system, once the compliance baseline is deployed you can decide if you need to get alerts when the compliance check falls below a specific percentage. To do this you must perform the following task:

1. In the Configuration Manager console, choose the Assets And Compliance workspace.
2. Under the Overview section, expand Compliance Settings.
3. Select Configuration Baselines.
4. In the right section select Microsoft Calculator Plus - Check; right-click and select Properties.
5. Click the Deployment tab.
6. Select the deployed collection and click Edit.
7. Click Generate An Alert, as shown previously in Figure 14.16.
8. Set the compliance percentage to 95.
9. Click OK twice.

This will generate the alert configuration on the Monitoring workspace, should less than 95 percent of the systems in the targeted collection be noncompliant.

Compliance Settings Reporting

After a short period of time you should be able to run several of the reports included with Configuration Manager for compliance and settings management. These reports can be customized to suit your needs, or you can build your own reports if they don't provide the level of detail you require. Reports are located in the Monitoring workspace, under Overview ➢ Reporting ➢ Reports; in the search criteria look for Compliance And Settings Management. The current list of reports is as follows:

- Compliance history of a configuration baseline
- Compliance history of a configuration item
- Details of compliant rules of configuration items in a configuration baseline for an asset

- Details of conflicting rules of configuration items in a configuration baseline for an asset
- Details of errors of configuration items in a configuration baseline for an asset
- Details of non-compliant rules of configuration items in a configuration baseline for an asset
- Details of remediated rules of configuration items in a configuration baseline for an asset
- List of assets by compliance state for a configuration baseline
- List of assets by compliance state for a configuration item in a configuration baseline
- List of rules conflicting with a specified rule for an asset
- List of unknown assets for a configuration baseline
- List of unknown assets for a configuration item
- Rules and errors summary of configuration items in a configuration baseline for an asset
- Summary compliance by configuration baseline
- Summary compliance by configuration items for a configuration baseline
- Summary compliance by configuration policies
- Summary compliance of a configuration baseline for a collection

Importing Configuration Packs

In this section you will learn how to implement a configuration pack from the Security Compliance Manager tool. This tool has different baselines, and each of the baselines can be exported to ConfigMgr and later or imported as Compliance Settings data.

What Is Security Compliance Manager?

Microsoft Security Compliance Manager provides security configuration recommendations from Microsoft, centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization's ability to efficiently manage the security and compliance process for the most widely used Microsoft products.

To download this tool, go to

```
http://www.microsoft.com/download/en/details
.aspx?displayLang=en&id=16776
```

To learn more about this tool, go to

```
http://technet.microsoft.com/en-us/library/cc677002.aspx
```

Figure 14.19 shows the Security Compliance Manager console focused on Internet Explorer 9 Computer Security Compliance. As an example, to import the Internet Explorer 9 configuration pack, perform the following procedure:

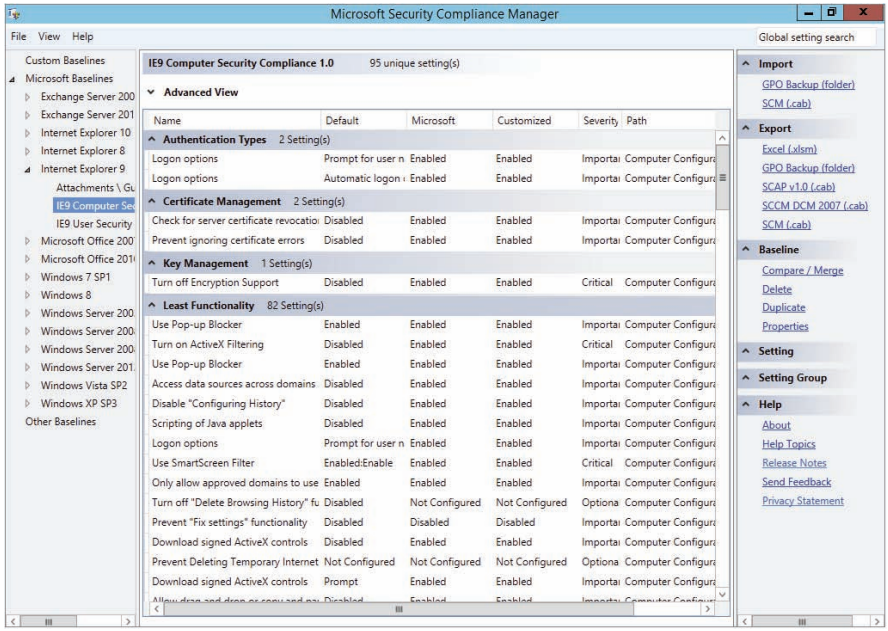


FIGURE 14.19
Microsoft Security Compliance Manager

1. Download Security Compliance Manager from the Microsoft Download site.
2. Install Security Compliance Manager.
3. Confirm that the product has been installed and all the baselines have downloaded it.
4. Launch the Security Compliance Manager tool.
5. For the Microsoft baseline select Internet Explorer 9.
6. For Internet Explorer 9 select IE 9 Computer Security Compliance.
7. In the right section the Export option will be enabled; click SCCM DCM 2007 (.cab).

   The Export to SCCM DCM 2007 dialog box will open.

   Note: Even though it says SCCM DCM 2007, this works great with ConfigMgr 2012 R2. On the new version of Security Compliance Manager, this should be updated.
8. Save the `.cab` file to a known location.
9. Open the Configuration Manager console.
10. Choose the Assets And Compliance workspace.
11. In the navigation pane, expand Compliance Settings, and then click Configuration Items.
12. In the navigation pane, right-click Configuration Baselines.
13. Choose Import Configuration Data.

The Import Configuration Data Wizard will appear, as shown in Figure 14.20.

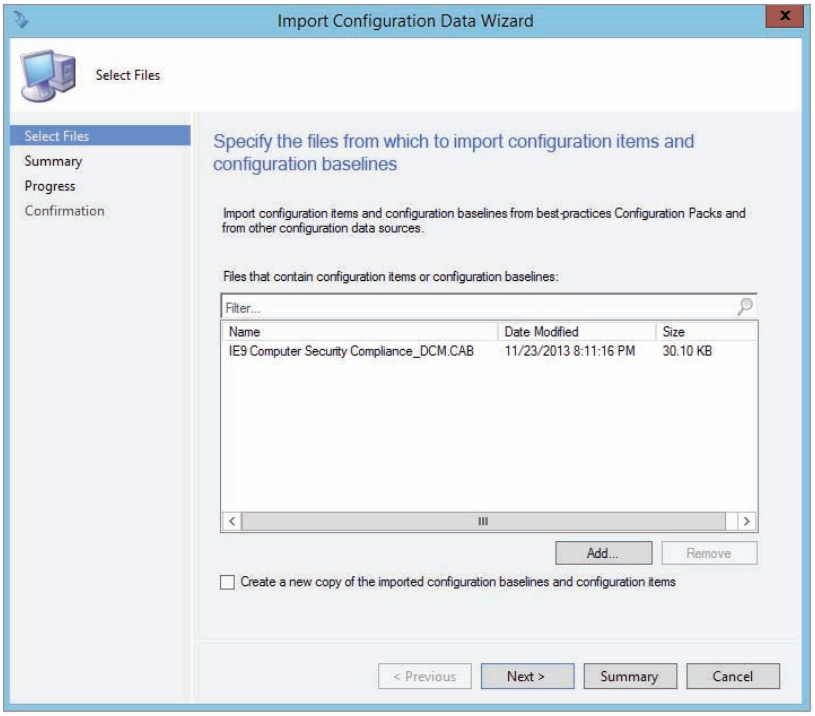


FIGURE 14.20
Import Configuration Data Wizard - Select Files page

14. Click Add.
15. The Open dialog box will appear; locate the file saved in step 8 and click Open.
16. Click Next. The import will analyze the `.cab` file.

    The Import Configuration Data Wizard Summary page will list one configuration baseline and six configuration items.
17. Click Next.

    The Import Configuration Data Wizard will complete at this point. Your Confirmation screen should look like the one in Figure 14.21. You can close the wizard.

Now that you have imported the configuration data to Configuration Manager's Compliance Settings, you can deploy this baseline to any collection and evaluate the current compliance state for Internet Explorer 9. This will also give you a better idea of how to use Compliance Settings and the configuration items.

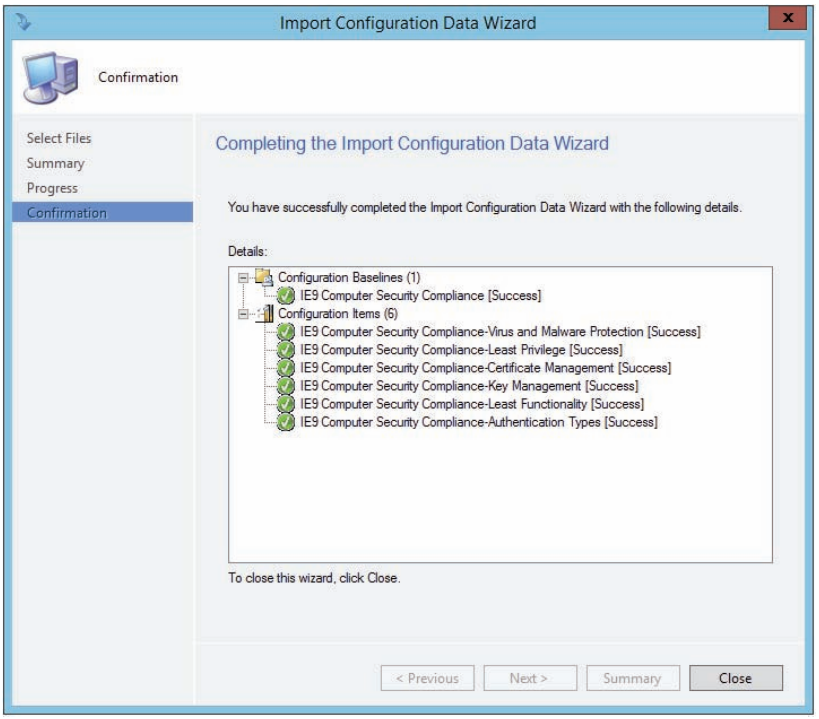


FIGURE 14.21
Import Configuration Data Wizard - Confirmation page

User Data and Profiles

User data and profiles configuration items contain settings that control how users in your hierarchy manage folder redirection, offline file, and roaming profiles on computers that run Windows 8 and Windows 8.1. You can deploy them to a collection of users and then monitor their compliance from the Monitoring node of the ConfigMgr console. Unlike other configuration items, you do not add these to configuration baselines before you deploy them. You can deploy them directly with the Deploy User Data and Profiles Configuration Policy dialog, as shown in Figure 14.22.

The following are examples of user data and profiles configuration items you can manage in ConfigMgr 2012 R2:

- Redirect a user's `Documents` folder to a network share.
- Ensure that specified files stored on the network are available on a user's computer when the network connection is unavailable.
- Configure which files in a user's roaming profile are synchronized with a network share when the users logs on and off.

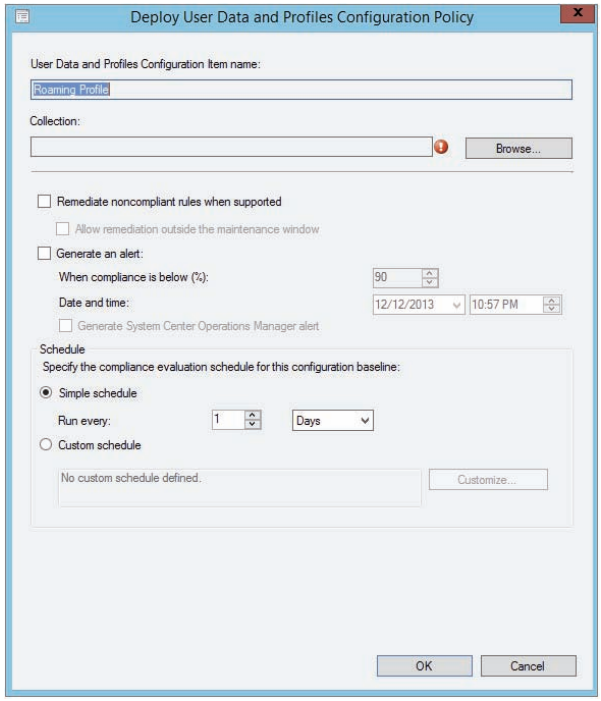


FIGURE 14.22
Deploy User Data And Profiles Configuration Policy dialog

Use the following steps to create a user data and profiles configuration item in ConfigMgr:

1. Open the ConfigMgr console and select Assets and Compliance ➢ Overview.
2. Choose Compliance Settings ➢ Users Data And Profiles. Right-click and select Create User Data And Profiles Configuration Item.
3. On the wizard, as shown in Figure 14.23, enter the information requested and select the appropriate check boxes:
   a. Name: Enter the name of this configuration item.
   b. Description: Enter details about this CI.
   c. Folder Redirection: Enable this check box if you are going to configure it as folder redirection.
   d. Offline Files: Enable this check box if you plan to configure offline files.
   e. Roaming User Profiles: Enable this check box if you want to configure roaming user profiles.
4. Click Next to go to the Folder Redirection step, shown in Figure 14.24. Specify how you want the client computers of users who receive this configuration item to manage folder redirection. You can configure settings for any device the user logs onto or for only the user's primary devices. This section will be available only if you checked the Folder Redirection box on the previous screen.

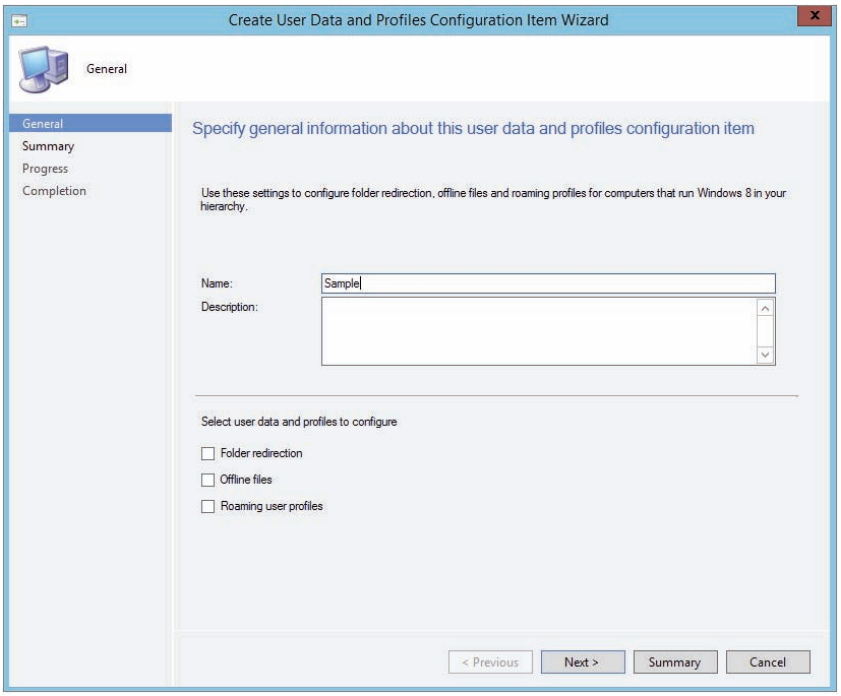


FIGURE 14.23
Create User Data And Profiles Configuration Item Wizard

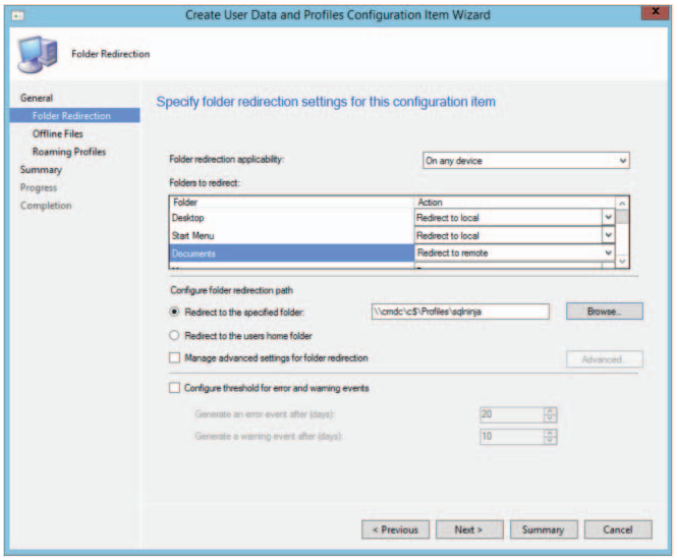


FIGURE 14.24
Create User Data And Profiles Configuration Item Wizard - Folder Redirection screen

5. Click Next to go to the Offline Files step, shown in Figure 14.25. You can enable or disable the use of offline files for users who receive this configuration item and configure settings for the behavior of the offline files. This section will appear only if you checked the Offline Files box on the initial screen shown in Figure 14.23.

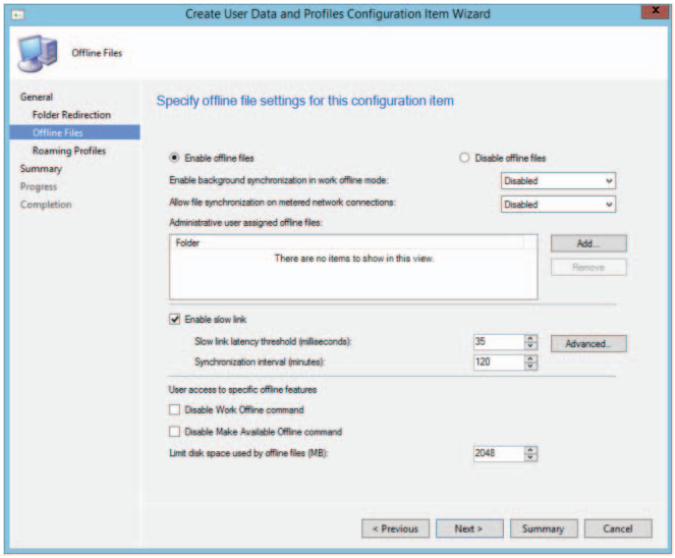


FIGURE 14.25
Create User Data And Profiles Configuration Item Wizard - Offline Files screen

6. Click Next to go to the Roaming Profiles step, shown in Figure 14.26. You can configure whether roaming profiles are available on computers that the users log onto and also configure further information about how these profiles behave. This section will appear only if you checked the Roaming Profiles box shown in Figure 14.23.

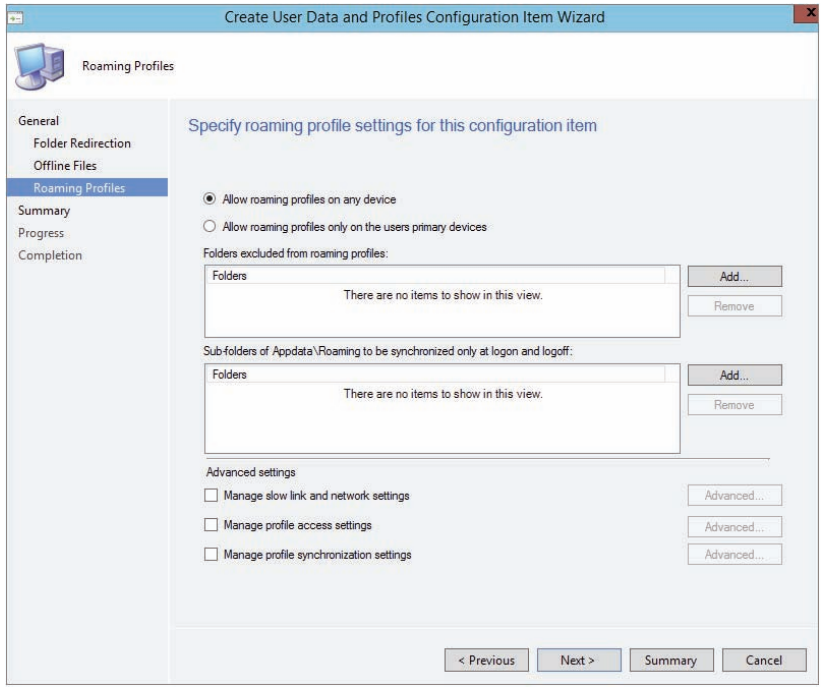


FIGURE 14.26
Create User Data And Profiles Configuration Item Wizard - Roaming Profiles screen

7. Click Next to go to the Summary page, as shown in Figure 14.27. On this screen you can review the actions that are going to be taken and then click Next to create the configuration item.

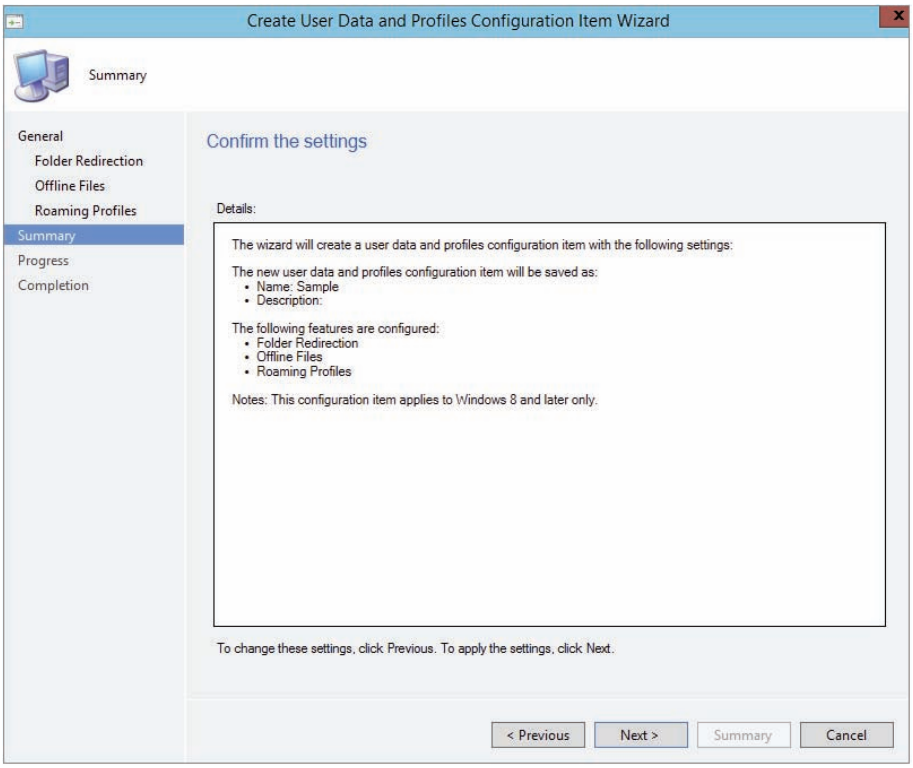


FIGURE 14.27 Create User Data And Profiles Configuration Item Wizard - Summary screen

8. Once you have completed the wizard, the New User Data And Profiles configuration item is shown in the User Data and Profiles node of the Assets and Compliance workspace. From here you can just deploy it to the desired collection.

Remote Connection Profiles

Remote connection profiles in System Center 2012 R2 Configuration Manager provide a set of tools and resources to help you create, deploy, and monitor remote connection settings to devices in your organization. By deploying these settings, you minimize the effort that end users require to connect to their computers on the corporate network. Use remote connection profiles in ConfigMgr 2012 R2 to allow users to remotely connect to work computers when they are not connected to the domain or if their personal computers are connected over the Internet.

Remote connection profiles let you deploy remote desktop connection settings to users in the ConfigMgr hierarchy. Users can then use the company portal to access any of their primary work computers through remote desktop by using the remote desktop connection settings

provided by the company portal. Windows Intune is required if you want users to connect to their work PCs by using the company portal.

In order to configure remote connection profiles, you need to create a remote connection profile:

1. In the Configuration Manager console, select the Assets And Compliance workspace.
2. Expand Compliance Settings.
3. Right-click Remote Connection Profiles and click Create Remote Connection Profile. The Create Remote Connection Profile Wizard will start, as shown in Figure 14.28.

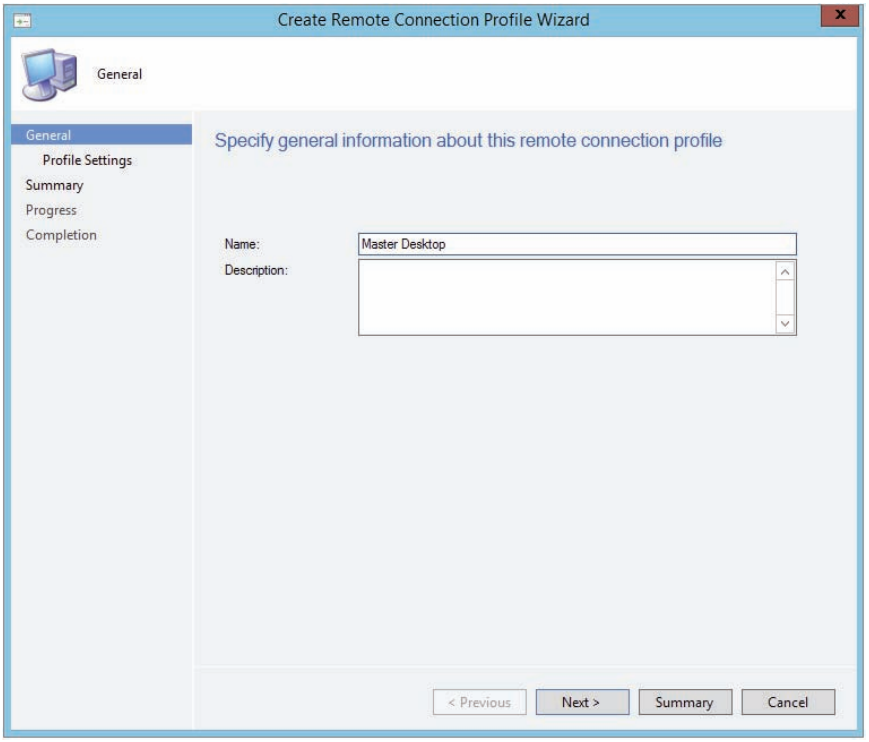


FIGURE 14.28
Create Remote Connection Profile Wizard - General page

4. Once you're in the Create Remote Connection Profile Wizard, enter the name of the remote connection profile and click Next.
5. On the Profile Settings screen, you will need to provide the full name and port of the Remote Desktop Gateway server, as shown in Figure 14.29.
6. Select Enabled or Disabled for each of the connection settings as required by your company policies.

   Note that all three items under Connection Settings must be set to either Enabled or Disabled. They must all match, regardless of which setting you choose to use.

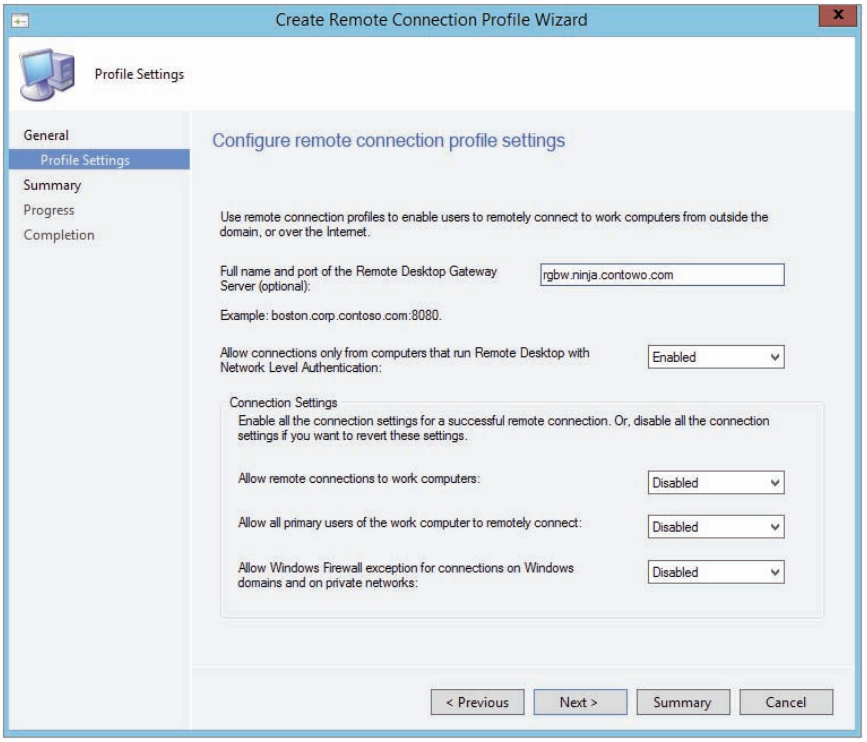


FIGURE 14.29
Create Remote Connection Profile Wizard - Profile Settings page

7. When all settings are configured, click Next.
8. The Summary page will be displayed. Click Next to create the remote connection profile and then Close to complete the Create Remote Connection Profile Wizard.

Company Resource Access

The Company Resource Access feature of System Center 2012 R2 Configuration Manager provides a set of tools and resources that enable you to give users in your organization access to data and applications from remote locations. This new feature allows you to create certificate, VPN, and Wi-Fi profiles in ConfigMgr and deploy them to users or device collections. To create each of these profiles you need to access the Compliance Settings section of the console, as shown in Figure 14.30.

Certificate Profiles

Certificate profiles provide a set of tools and resources to help provision computers in your organization with the certificates that users require to connect to various company resources. Certificate Profiles in System Center 2012 Configuration Manager works with Active Directory Certificate Services and the Network Device Enrollment service role to provision authentication certificates for managed devices so that users can seamlessly access company resources. This setting is available on the Company Resource Access area of Compliance Settings, as shown in Figure 14.31.

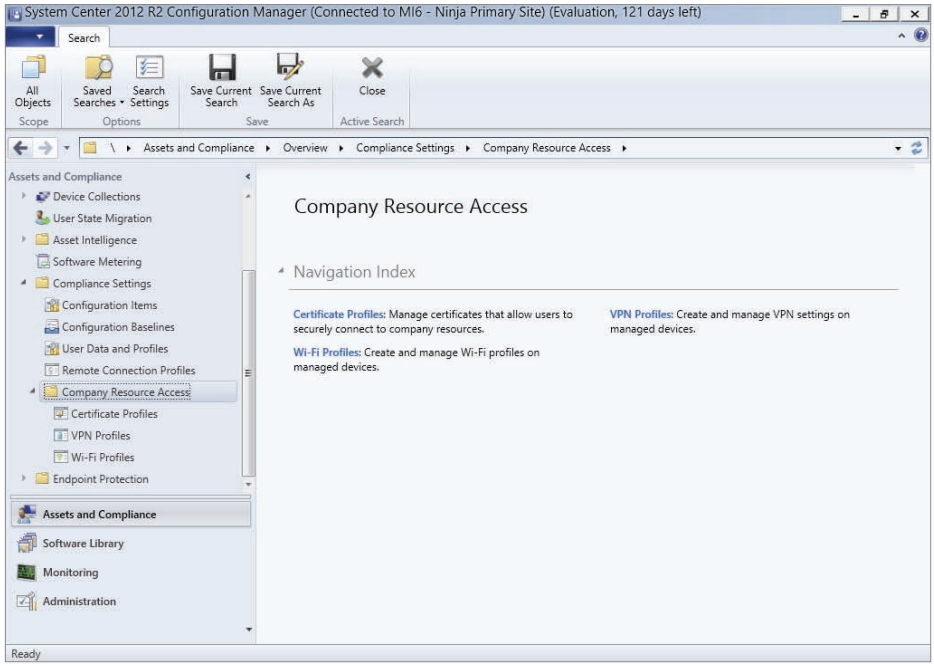


FIGURE 14.30
Company Resource Access

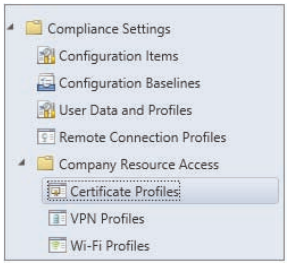


FIGURE 14.31
Company Resource Access - Certificate Profiles

Certificates Profiles provide the following management capabilities:

- Certificate enrollment and renewals from an enterprise certification authority for devices that run iOS 5/6/7, Windows 8.1/RT 8.1, and Android. These certificates can then be used for Wi-Fi and VPN connections.
- Deployment of trusted root CA certificates and intermediate CA certificates to configure a chain of trust on devices for VPN and Wi-Fi connections when server authentication is required.
- Monitor and report on the installed certificates.

Now that you understand what Certificate Profiles is used for, let's configure a certificate profile and deploy it to users or device collections.

To create the certificate profile, follow these steps:

1. In the Configuration Manager console, navigate to the Assets And Compliance workspace.
2. Expand Compliance Settings ➢ Company Resource Access.
3. Right-click Certificate Profiles and select Create Certificate Profile.
4. The Create Certificate Profile Wizard will be displayed, as shown in Figure 14.32.

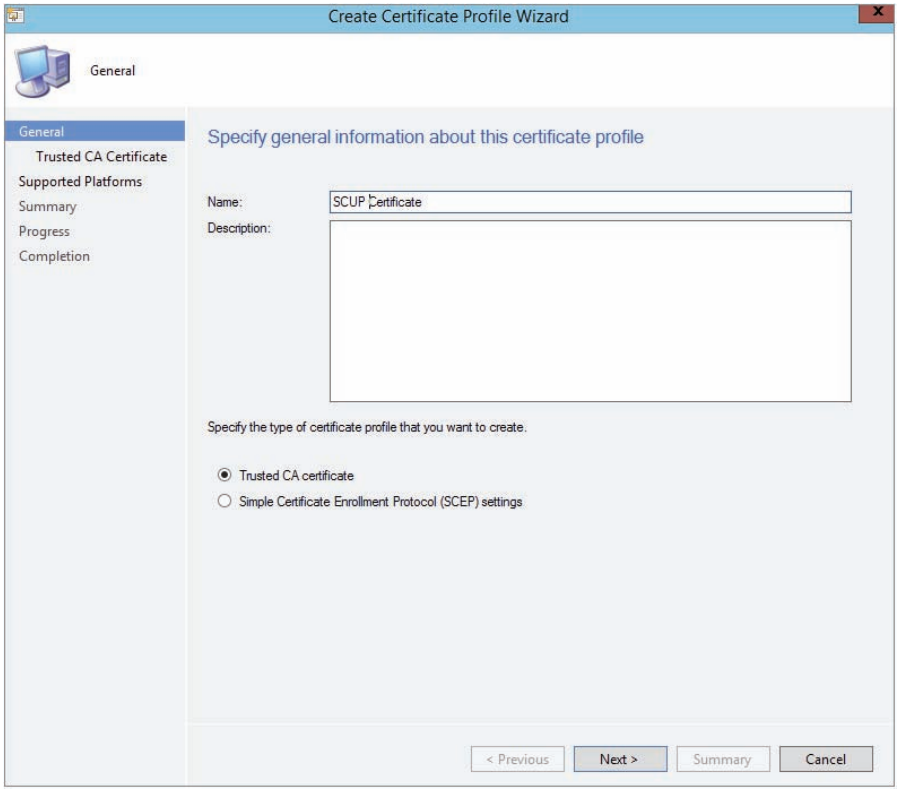


FIGURE 14.32 Create Certificate Profile Wizard - General page

5. Enter the name of the certificate profile.
6. Select either Trusted CA Certificate or Simple Certificate Enrollment Protocol (SCEP) Settings.
7. Click Next to continue the wizard.
8. Click Import, as shown in Figure 14.33, and select the certificate that you want to deploy.
9. Click Next to go to the Supported Platforms page, as shown in Figure 14.34.

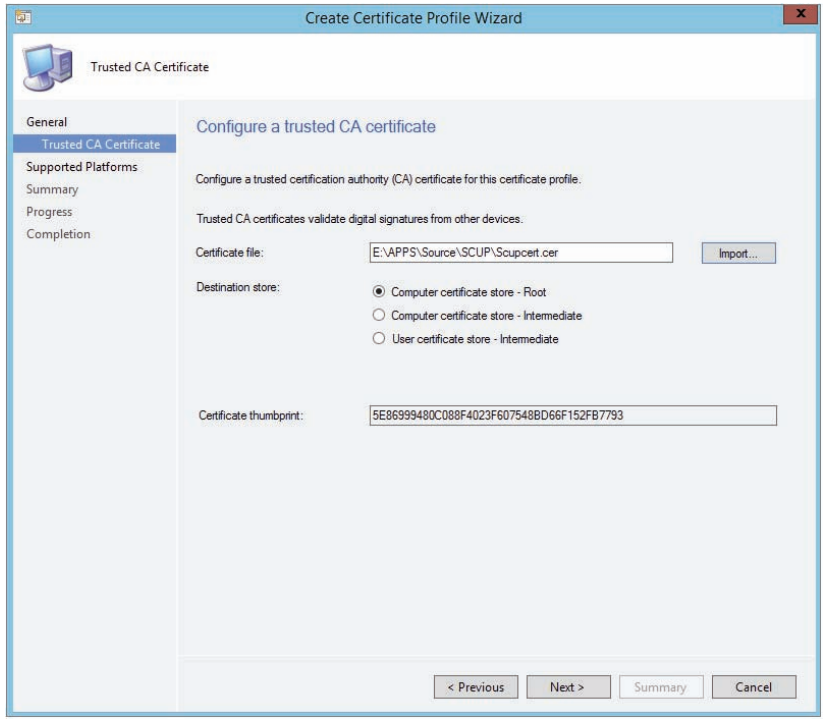


FIGURE 14.33
Create Certificate Profile Wizard - Trusted CA Certificate page

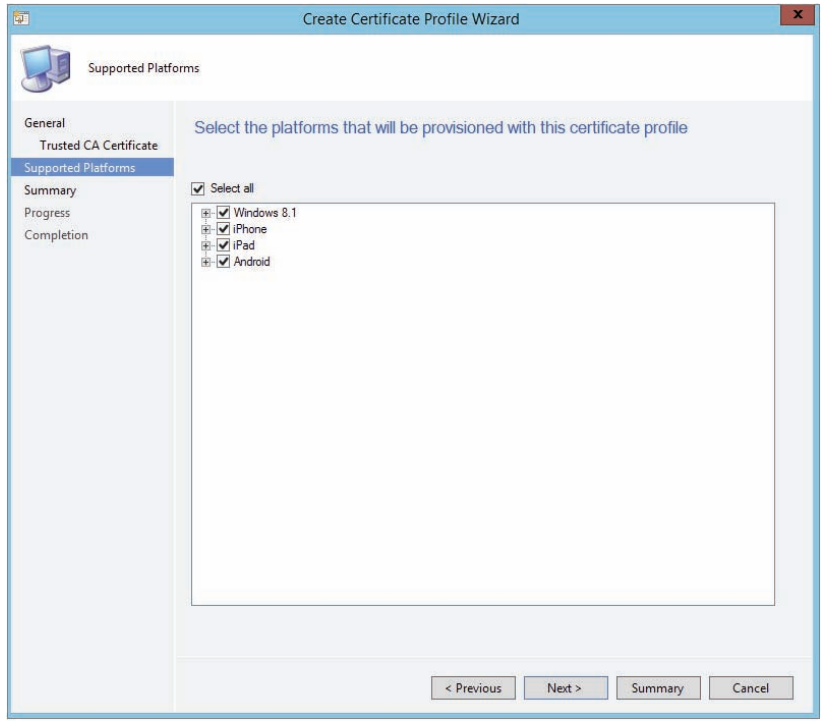


FIGURE 14.34
Create Certificate Profile Wizard - Supported Platforms page

10. Select all the OS versions that you need for the certificate, and then click Next.
11. Review the Summary page, and click Next.
12. When the configuration is complete, review the Completion screen, as shown in Figure 14.35; then click Close to complete the Create Certificate Profile Wizard.

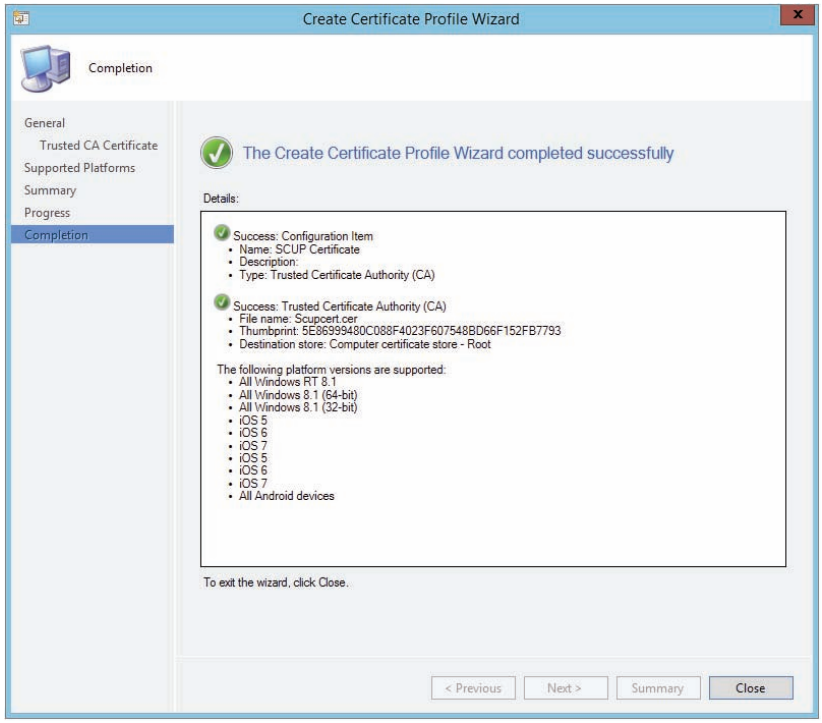


FIGURE 14.35
Create Certificate Profile Wizard - Completion page

13. Your certificate profile should now be visible on the system.

Once the certificate profile is created, you can deploy it to a user or a device collection of your choosing.

VPN Profiles

You use VPN profiles in ConfigMgr 2012 R2 to deploy VPN settings to users in your organization. By deploying these settings, you can minimize the effort required to connect to the resources of the company network. With a new VPN profile you can easily configure any devices on your organization that may need this setting to connect to the network. You can create this profile to support Windows 8.1, Windows RT, and iOS 5, 6, and 7.

A VPN profile can include a wide range of security settings, including certificates for server validation and client authentication that have been provisioned by ConfigMgr certificate profiles.

To create a VPN profile, follow these steps:

1. Open the ConfigMgr console and choose the Assets And Compliance workspace.
2. Expand Compliance Settings ➢ Company Resource Access.
3. Right-click VPN Profiles and click Create VPN Profiles.
4. The Create VPN Profile Wizard will appear, as shown in Figure 14.36.

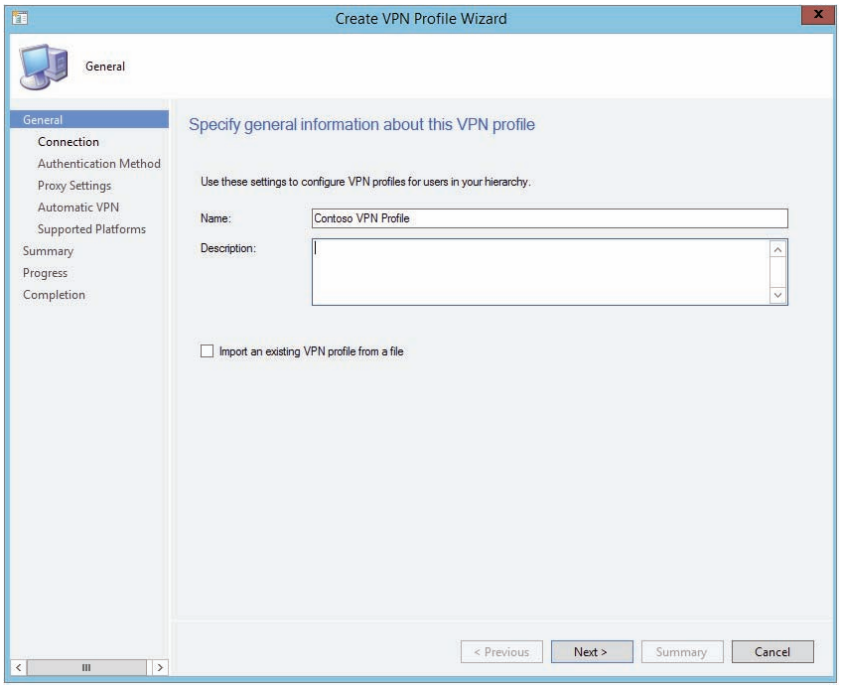


FIGURE 14.36
Create VPN Profile Wizard - General page

5. Enter the name and a description for the VPN profile.
6. Check Import An Existing VPN Profile From A File, if you already have these details saved. Otherwise, click Next.
7. On the Connection page, as shown in Figure 14.37, select the right connection type and server list for your environment.
8. Click Add to specify a VPN server. Enter a friendly name and the IP address of the server or FQDN. Once you've entered all the information, click Next.
9. Select the authentication method that you are going to use for this VPN connection, as shown in Figure 14.38.

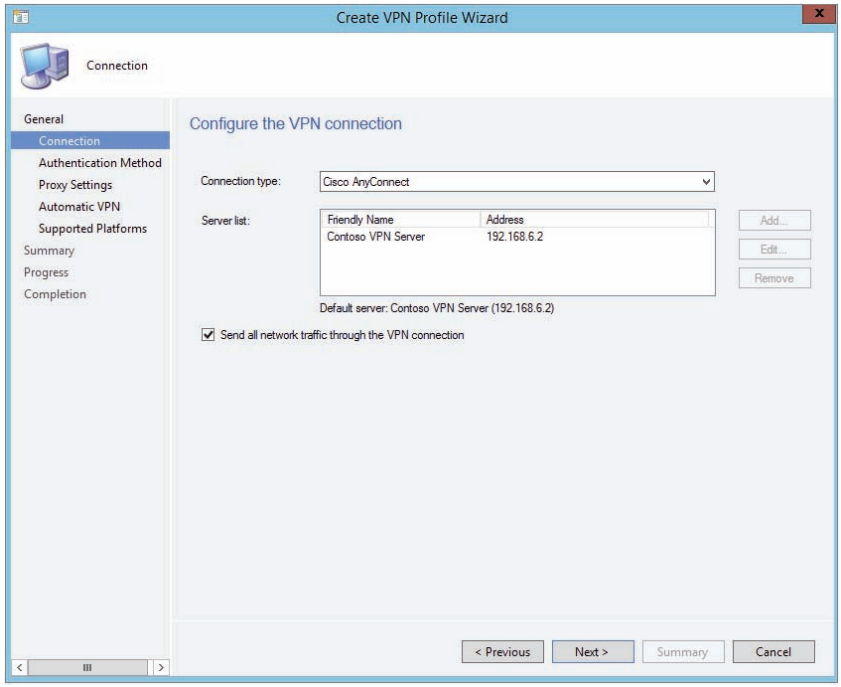


FIGURE 14.37
Create VPN Profile Wizard - Connection page

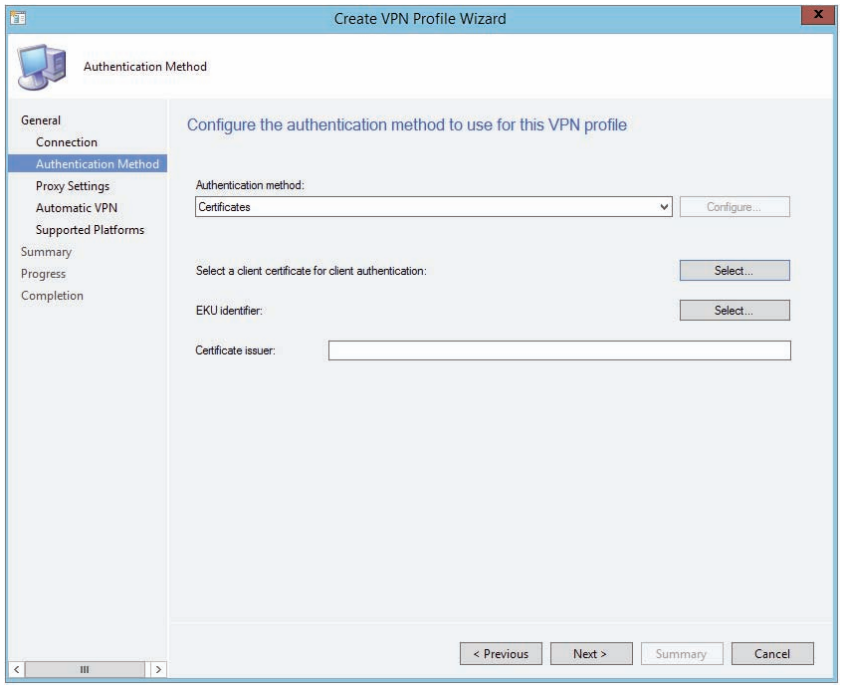


FIGURE 14.38
Create VPN Profile Wizard - Authentication Method page

10. Click Next once you've configure the right authentication method.
11. Configure the proxy setting that is needed for this VPN profile, as shown in Figure 14.39.

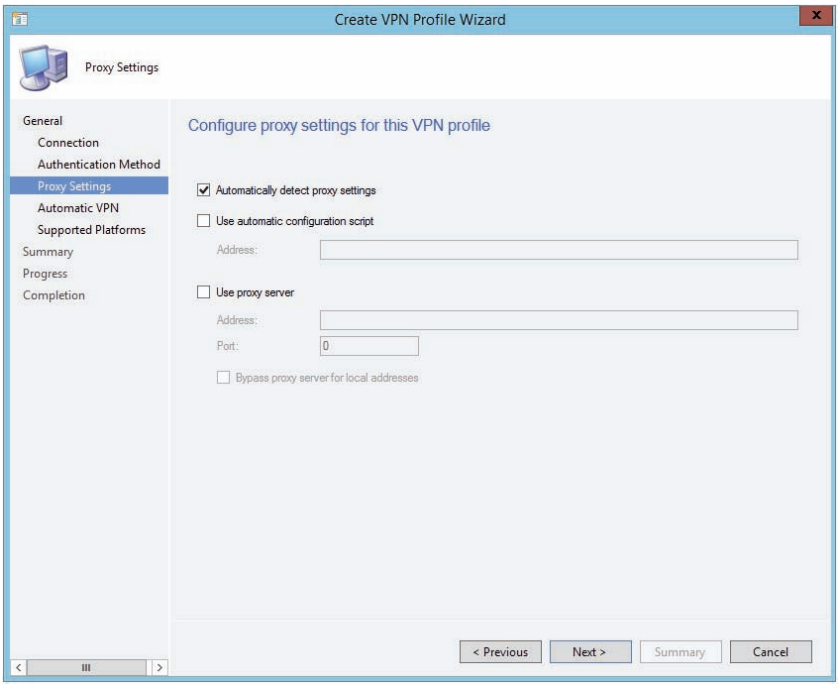


FIGURE 14.39
Create VPN Profile Wizard - Proxy Settings page

12. Click Next once you've configured the proxy settings appropriately.
13. On the Automatic VPN page, shown in Figure 14.40, you need to indicate which requests you wish to trigger a VPN connection to. Check Enable VPN On-Demand, and then enter the VPN suffixes in order to trigger an automatic VPN connection. All settings on this page are optional. Click Next to move to the next page in the wizard.
14. Select the supported platforms for this VPN profile, as shown in Figure 14.41, and then click Next.
15. On the Summary screen, review all settings to ensure every configuration you wanted is set up; then click Next.
16. Click Close to complete the configuration of your VPN profile.

VPN profiles can save your users lots of time. Make sure you configure all the settings that are needed for the VPN profile before deploying it to your production devices.

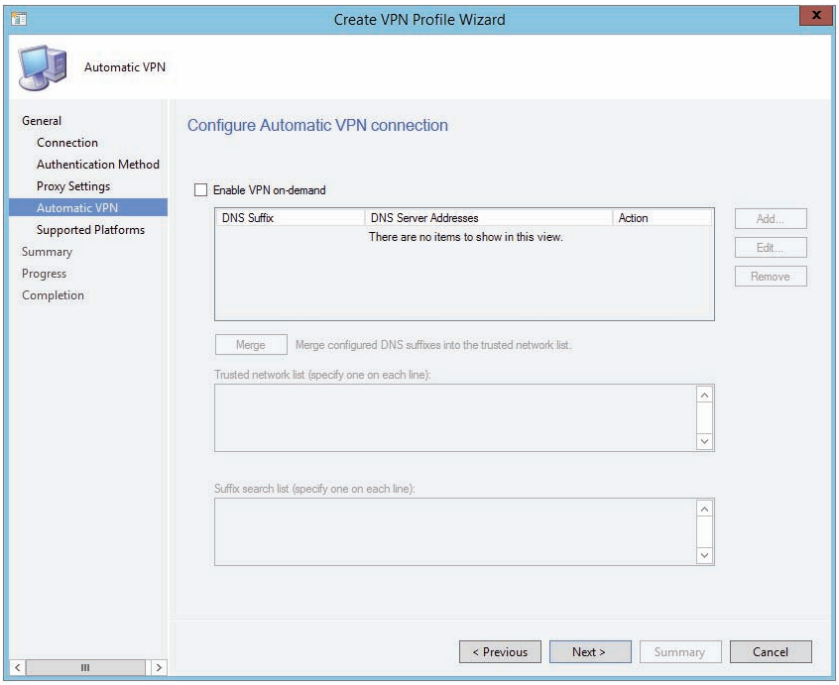


FIGURE 14.40
Create VPN Profile Wizard - Automatic VPN page

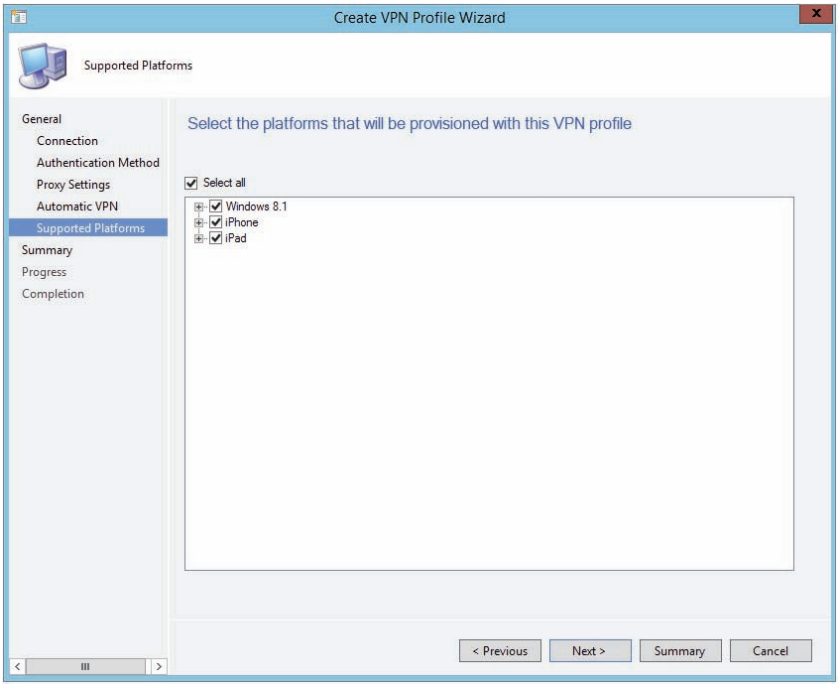


FIGURE 14.41
Create VPN Profile Wizard - Supported Platforms page

Wi-Fi Profiles

In ConfigMgr 2012 R2 you can configure Wi-Fi profiles and deploy them to your users and device collections to ensure the Wi-Fi settings are correct. This will help you minimize the end-user effort required to connect to the corporate wireless network.

If you install a new Wi-Fi network and you want to provision it to all the devices in your organization, you can create a Wi-Fi profile containing the settings necessary to connect to the new Wi-Fi network. Then you can deploy this profile to all users or devices. The new Wi-Fi profile supports the following device types: Windows 8.1 and RT, iOS 5, 6, and 7, as well as Android devices that run version 4.

Follow these steps to configure a Wi-Fi profile:

1. Open the ConfigMgr console and choose the Assets and Compliance workspace.
2. Expand Compliance Settings ➢ Company Resource Access.
3. Right-click Wi-Fi Profiles and select Create Wi-Fi Profiles.
4. The Create Wi-Fi Profile Wizard will appear, as shown in Figure 14.42.

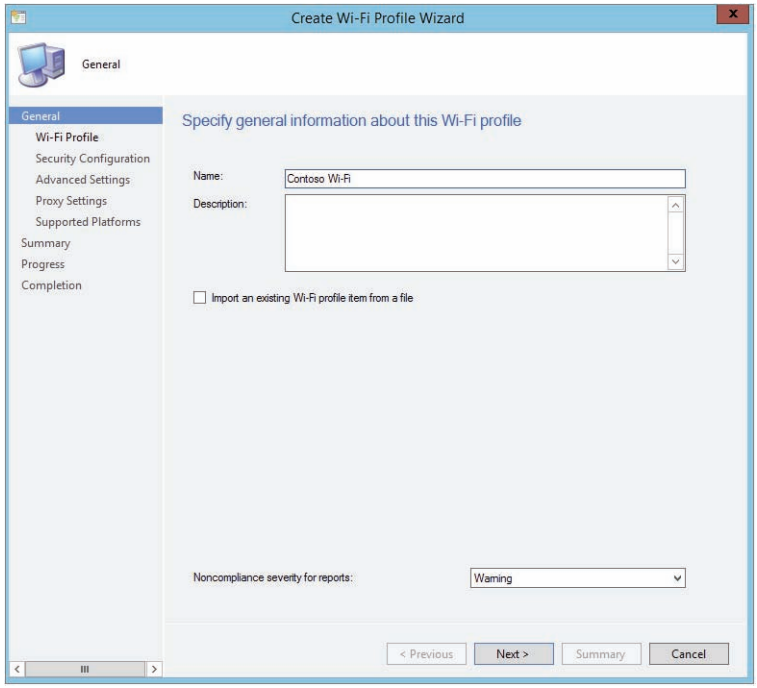


FIGURE 14.42 Create Wi-Fi Profile Wizard - General page

5. Enter the name and a description for the Wi-Fi profile. If you have an existing Wi-Fi profile in a file, you can select to import it and click Next.
6. As shown in Figure 14.43, enter the network name and SSID. Select Connect Automatically When This Network Is In Range if you need this to be the default Wi-Fi profile; otherwise leave all boxes unchecked and click Next.
7. On the Security Configuration page, select a security type, as shown in Figure 14.44. Click Next once you finish configuring the proper security for the Wi-Fi profile.

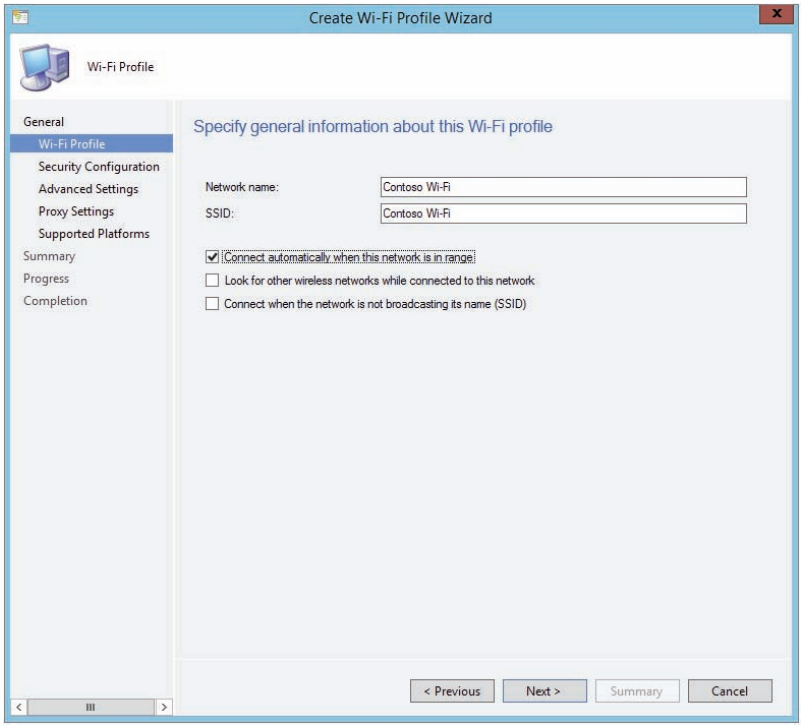


FIGURE 14.43
Create Wi-Fi Profile Wizard - Wi-Fi Profile page

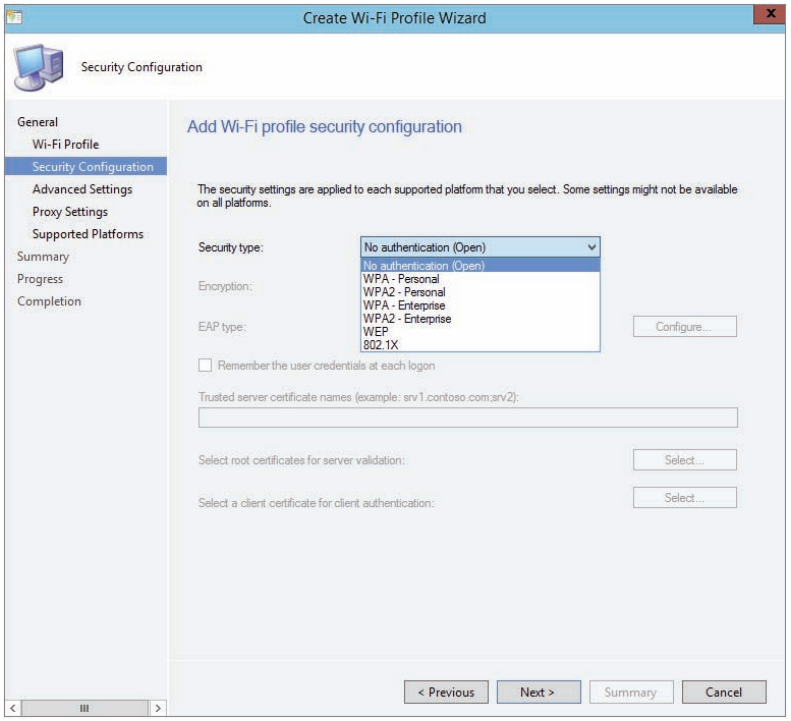


FIGURE 14.44
Create Wi-Fi Profile Wizard - Security Configuration page

8. On the Advanced Settings page, configure additional details, as shown in Figure 14.45, and then click Next.

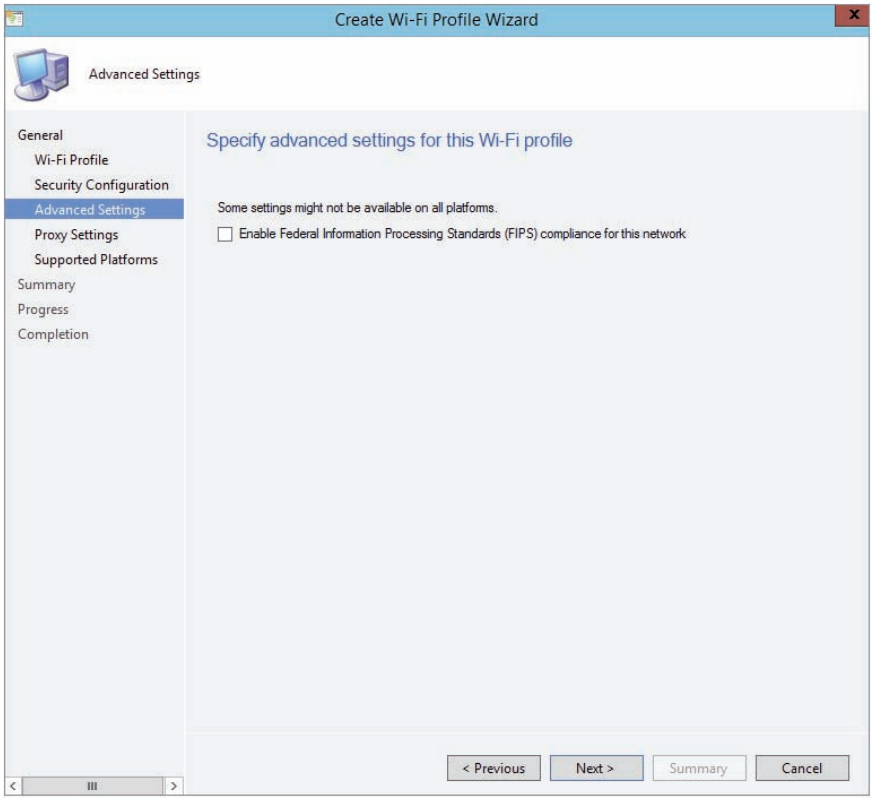


FIGURE 14.45
Create Wi-Fi Profile Wizard - Advance Settings page

9. On the Proxy Settings page, enter the proxy information for this Wi-Fi profile if needed. No settings are required, as shown in Figure 14.46. Click Next to continue.
10. On the Supported Platforms page, select the devices required for your environment or just click Select All, and then click Next.
11. On the Summary page, review the information, making sure to validate the configuration before you deploy this profile.

As you have seen, using the Wi-Fi Profiles feature, it is very easy to configure and manage the process of deploying Wi-Fi profiles to ConfigMgr users and devices.

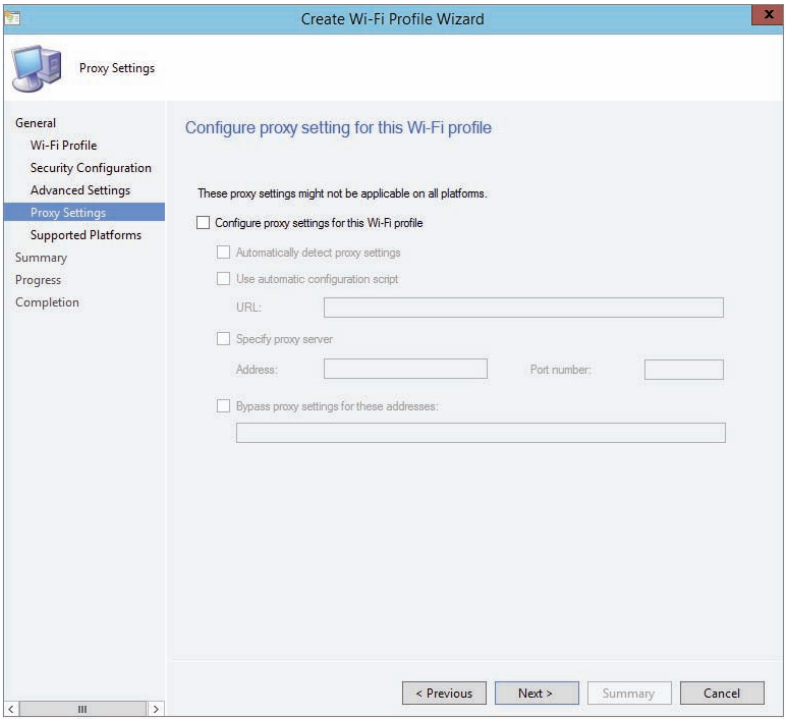


FIGURE 14.46
Create Wi-Fi Profile Wizard - Proxy Settings page

The Bottom Line

Enable the client settings. Until the client settings are enabled for your Configuration Manager clients, your clients will not evaluate any of the configuration baselines. This is the first step in using Compliance Settings to validate client settings.

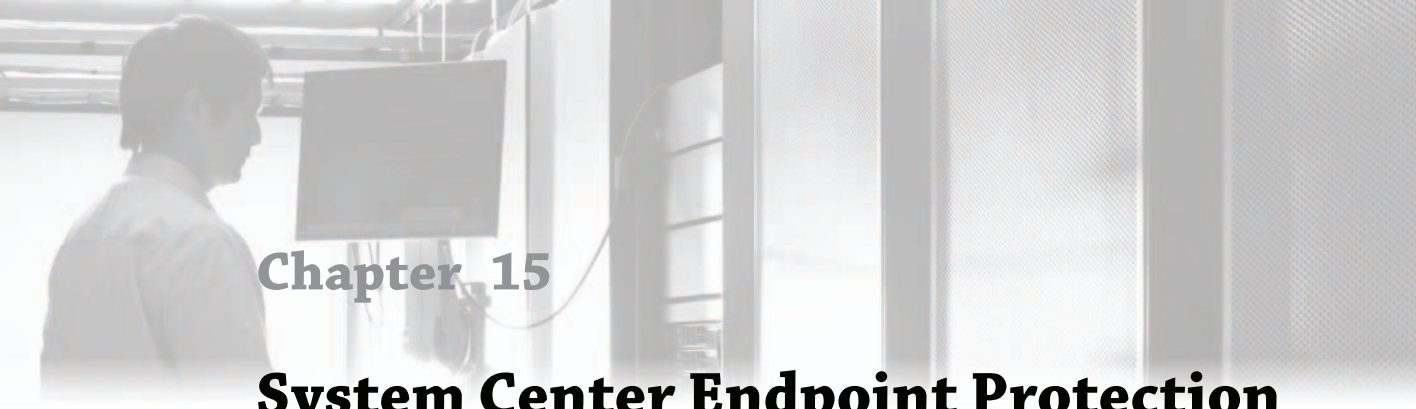
Master It Enable Compliance Settings for the Configuration Manager clients.

Create configuration items. Configuration items are the pieces that make up a configuration baseline. There are a number of different configuration item types in Configuration Manager, and depending on the type you choose to create, you are presented with certain options when creating your configuration item. The steps to create configuration items were covered in the first part of this chapter, and they included several examples of how to create the different types of configuration items.

Master It Create a configuration item for an application that checks a registry string value.

Define a configuration baseline. This is where you take one or more of the CIs and put them into a package that the Configuration Manager client downloads and at the scheduled time validates by checking the CIs against the computer. The Configuration Manager client then reports the outcome of those checks back to Configuration Manager, where you can then run reports to see if your clients are within the specified configuration. These steps were covered in the last section of the chapter.

Master It Assemble a configuration baseline with one or more configuration items you have created.



Chapter 15

System Center Endpoint Protection

System Center Configuration Manager 2007 provided the ability to integrate with Microsoft Forefront Endpoint Protection 2010. Forefront Endpoint Protection (FEP) is Microsoft's industry-leading security and antimalware product, and the integration with Configuration Manager 2007 allowed administrators to easily manage and control its configuration.

The Forefront Endpoint Protection product has been updated for 2012, and the new version is called System Center 2012 Endpoint Protection (SCEP). As you will see in this chapter, the integration between Endpoint Protection and Configuration Manager is carried forward and greatly enhanced in the System Center 2012 versions of the products.

In this chapter, you will learn to

- Differentiate between FEP and SCEP
- Deploy and configure the System Center 2012 Endpoint Protection site system and client
- Create and assign an SCEP policy

Differences between FEP and SCEP

Before taking a closer look at System Center 2012 Endpoint Protection, let's take a moment to review some of the key differences between Forefront Endpoint Protection 2010 and System Center 2012 Endpoint Protection:

- FEP used two separate databases to store data, FEP_DB and FEP_DW. SCEP uses the ConfigMgr site database to store all data.
- FEP required a separate client to be deployed and installed on each managed computer. SCEP includes the endpoint client software as part of the ConfigMgr 2012 client install media, and the SCEP client is enabled and configured in the ConfigMgr 2012 console.
- FEP had a delay between when a malware event occurred at a client, such as virus detection, and when that information was made available to the ConfigMgr 2007 administrator. ConfigMgr 2012 has new internal processes that work to greatly reduce the time that elapses between the event and the alerting and reporting.
- Delegating the administration of FEP was a challenge in ConfigMgr 2007. In ConfigMgr 2012, the role-based security model allows the ConfigMgr administrator to easily delegate the SCEP-related functions to a specific person or group without providing those users with access to other areas of ConfigMgr.

What Is Malware?

We will use the term *malware* a great deal in this chapter, so it's probably a good idea to define that word.

Malware is short for *malicious software*, which is basically software, code, or scripts that are typically designed to perform invasive, destructive actions on a computer. Some malware attempts to delete files or corrupt the operating system, while others may attempt to steal personal or corporate data. Malware includes items such as computer viruses, worms, Trojan horses, adware, and some rootkits. Antimalware software (such as SCEP) is software designed to detect, block, and remove malware.

Additional Benefits of SCEP

Now that we have identified some of the key differences between the FEP 2010 and SCEP products, let's take a look at some of the additional benefits of the SCEP product. We will expand on these in the remainder of the chapter.

Deployment

The deployment and configuration of SCEP are managed in the ConfigMgr 2012 console. Because of the tight integration with ConfigMgr 2012, SCEP is easily deployable to environments of any size. The ConfigMgr administrator enables SCEP in ConfigMgr 2012 by deploying the new Endpoint Protection Point site system role, enabling the Endpoint Protection client, and then configuring the antimalware policies. SCEP also includes several policy templates that provide recommended antimalware configurations for standard workloads. These templates are generally ready to deploy but can be customized to meet the specific needs of the organization if needed. You can also export policies that were created in FEP 2010 and import them into SCEP.

Protection

SCEP provides ConfigMgr administrators with the ability to ensure that their computer infrastructure is safe and secure from malware attacks. The SCEP product protects the computer infrastructure by detecting and blocking malware and also by providing management of Windows Firewall. SCEP ensures that the computers are protected from many known exploits and vulnerabilities, and SCEP is backed by the Microsoft Security Response Center and the Microsoft SpyNet community. For more information on the Microsoft Security Response Center visit

```
http://www.microsoft.com/security/msrc
```

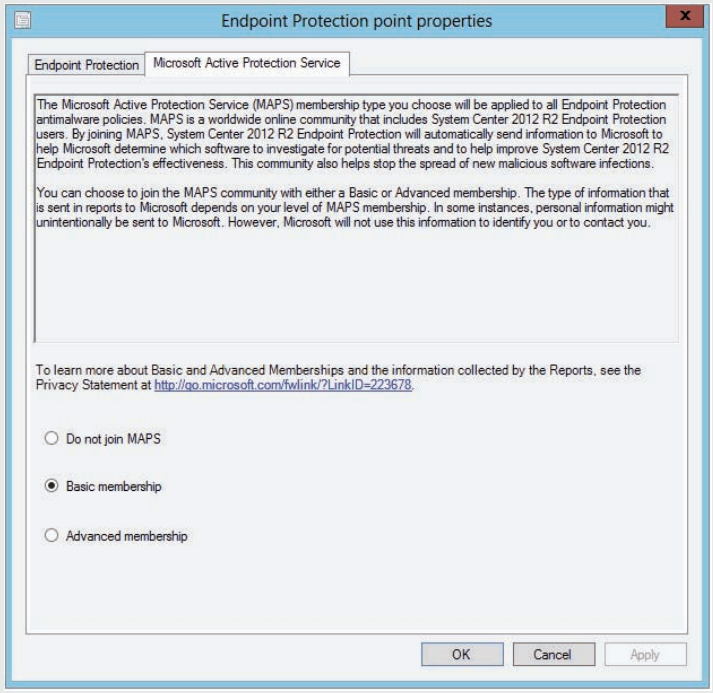
SpyNet Is Now MAPS

Before moving on, we should discuss the Microsoft Active Protection Service. In FEP 2010 this feature was referred to as Microsoft SpyNet but is now referred to as the Microsoft Active Protection Service (MAPS).

MAPS is a cloud-based service that allows the endpoint client on a computer to report data about programs that exhibit suspicious behavior to the Microsoft Malware Protection Center (MMPC). Once the data is submitted to the MMPC, it can be analyzed and researched by engineers. Once the data has been analyzed, information about the behavior can be included in a new definition update and deployed to computers around the world via FEP or SCEP. This feature is sometimes referred to as the Dynamic Signature Service.

When you configure the Endpoint Protection site system, you will need to define how MAPS should be configured for your environment.

As you can see in the following illustration, there are three available choices for the Microsoft Active Protection Service:



- Do not join MAPS

  If you choose this option, it means that information will not be sent from the managed computers to Microsoft. You will not be alerted if software that is currently unclassified is detected in the environment.

- Basic Membership

  If you choose the Basic Membership option, SCEP will submit information to Microsoft about potentially unsafe software or software that has not yet been analyzed for risks.

- Advanced Membership

  If you choose the Advanced Membership option, SCEP will submit more detailed information about detected software and will also alert you if software has been detected that has not yet been analyzed for issues or risks. This option also collects additional information from the computers, including IP address and operating system.

You can change the membership setting at any time by making the change in the Forefront Endpoint Protection site system properties. You can also override this sitewide setting with a custom antimalware policy if needed.

Monitoring

ConfigMgr 2012 includes several enhancements around the monitoring and the reporting of the health and status of the environment. This is especially true for the Endpoint Protection feature of ConfigMgr 2012.

One key improvement is the manner and speed in which endpoint protection activity (such as a malware event on a workstation) is sent to the site servers for monitoring purposes. In FEP 2010 there was some delay before malware outbreaks were made visible to the ConfigMgr administrator. The extent of that delay varied, depending on how FEP and ConfigMgr 2007 were configured, but with some scenarios it might have taken 30 minutes or more before the ConfigMgr administrator was aware of the malware activity.

In ConfigMgr 2012 a new mechanism has been implemented that greatly reduces the delay in getting endpoint malware activity data from the client to the site servers. This new client communication channel uses state messages to deliver malware activity information to the site server in almost real time. As a result, the ConfigMgr 2012 administrator will typically become aware of malware activity within just a few minutes of it taking place. ConfigMgr 2012 uses this channel for all endpoint-related operations as well as the Download Computer Policy client action. You will learn more about the fast channel later in the chapter.

Security

The role-based security model in ConfigMgr 2012 greatly simplifies the process of defining access for administrative users. The ConfigMgr 2012 security role that is related to the SCEP feature is the Endpoint Protection Manager. This security role provides the administrative user with the ability to create, modify, and delete security policies. Administrative users with this security role can also manage the security policies that are assigned to collections, monitor the status of SCEP, and execute remediation tasks on managed computers.

One possible use of this role is to assign it to the corporate IT security department and allow them to manage the configuration of SCEP without giving them access to other areas of ConfigMgr.

Now that you understand some of the features of System Center 2012 Endpoint Protection, let's take a closer look at the product.

Endpoint Protection Site System Role

System Center 2012 Configuration Manager introduces a new site system role, the Endpoint Protection Point site system role. This role must be installed and configured before you can use Endpoint Protection in ConfigMgr 2012. Also, the role must be installed at the top of the ConfigMgr 2012 hierarchy, which will be the Central Administration Site (CAS) if one exists. If the environment does not have a CAS, then the role will be installed on the standalone primary site.

Can SCEP Be Used in an Unmanaged Scenario?

Since you are reading this book, it is likely that you plan to use SCEP with ConfigMgr 2012 in a managed scenario and receive the many benefits of the integration between the two products.

However, SCEP can also be used in an *unmanaged* scenario, where ConfigMgr 2012 is not used to centrally administer, maintain, and monitor the configuration of SCEP. This scenario has some limitations but may be useful in environments where either ConfigMgr 2012 is not installed or the ConfigMgr client cannot be installed on computers.

In the unmanaged scenario, ConfigMgr 2012 is not available to deploy the SCEP clients and policies or update the SCEP definition files. An alternative is to use Active Directory Group Policy objects (GPOs) to deploy the SCEP client and policies and use Microsoft Update, Windows Server Update Services (WSUS), or the Microsoft Malware Protection Center (MMPC) to update the definition files. This same approach was available for FEP 2010, and Microsoft released a set of tools called Forefront Endpoint Protection 2010 Tools to assist with the configuration. It is possible that Microsoft will release a similar toolset for SCEP. One advantage of the GPO approach over the integrated ConfigMgr scenario is that group policies are dynamically merged when applied at the computer, allowing the administrator to maintain fewer group policies.

Another limitation of the unmanaged SCEP scenario is that you have no ability to receive real-time notification in the event of a malware outbreak in the environment, and you also have no ability to determine whether the SCEP clients are using outdated definition files. One possible exception is if the environment uses System Center 2012 Operations Manager (SCOM). If SCOM is in place, and the affected computers have the SCOM agent installed, the administrator may receive malware activity and outdated definition file status as SCOM alerts via an Endpoint Protection security management pack. A management pack was provided for FEP 2010 (Forefront Endpoint Protection 2010 Security Management Pack), and it's likely that Microsoft will provide a management pack for SCEP. However, SCOM is typically used only to monitor servers, and it's likely that your desktops and laptops will not have the SCOM agent installed.

As you can see, in some scenarios using SCEP in an unmanaged configuration may be useful, but the approach has some limitations. Also, you will need to contact your Microsoft account team or software reseller to determine the SCEP licensing requirements for this scenario.

The installation and configuration of the role are fairly straightforward:

1. In the Configuration Manager console, select Administration ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles.
2. Select the Central Administration Server (or the standalone primary site server), right-click, and select Add Site System Roles. The Add Site System Roles Wizard opens.
3. On the General page, specify the settings for the site system server. Click Next.
4. Select the proxy settings; then click Next.
5. On the next screen, select Endpoint Protection Point from the list of available roles and click Next. See Figure 15.1.
6. On the Specify Endpoint Protection License Page, accept the Endpoint Protection license terms and click Next.

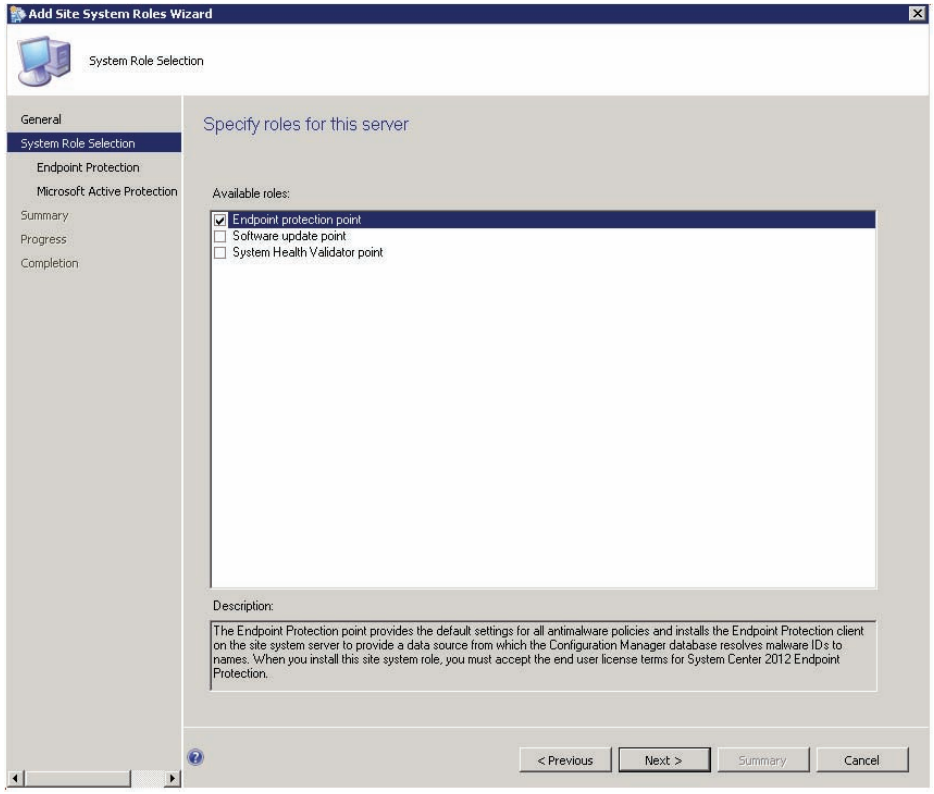


FIGURE 15.1 Selecting the Endpoint Protection Point role

The Endpoint Protection Client License

Note that you must accept the license agreement in order to install the Endpoint Protection Point role. As with FEP 2010, the Endpoint Protection client license is part of the Microsoft core Client Access License (CAL). However, the license for the Endpoint Protection site server is not part of the core CAL and has specific licensing requirements. Contact your Microsoft account team or software reseller for additional information on the licensing requirements for SCEP.

7. Choose the Print License Terms option if you would like to review the license terms before agreeing to them. Click Next.
8. On the Specify Microsoft Active Protection Service membership type window, choose the membership option you require for your environment and click Next.
9. On the Confirm Settings page, click Next and then click Close once the role has been successfully installed.
10. You can monitor the status of the installation of the role in the `EPMgr.log` and `EPSetup.log` files on the site server.

Show Me the Logs!

The SMS and ConfigMgr products have always had detailed, informative logs, and ConfigMgr 2012 is no different. The relevant logs for SCEP are discussed here:

On the SCEP Site System

The SCEP site system log files are in the standard location for ConfigMgr 2012 site server logs (`\Program Files\Microsoft Configuration Manager\Logs`), and there are three logs related to SCEP:

- `EPCtrlMgr.log` records information about the sync of malware threat data from the SCEP site system role to the ConfigMgr database.
- `EPMgr.log` monitors the status of the SCEP role.
- `EPSetup.log` records information about the installation of the SCEP role on the site server.

On the SCEP Clients

The SCEP client log files are located in `\Program Files\SMS_CCM\Logs` on the ConfigMgr 2012 site servers and in `\Windows\CCM\Logs` for ConfigMgr clients. There is one log related specifically to SCEP: `EndpointProtectionAgent.log`. This logs details the installation of the SCEP client and the application of antimalware policy.

Endpoint Protection Client Agent

Once the Endpoint Protection Point site system role has been enabled and configured, you need to enable and configure the System Center 2012 Endpoint Protection client agent. The installation media for the endpoint client is distributed to the managed devices as part of the ConfigMgr 2012 client install media. The name of the file is `SCEPInstall.exe`, and it can be found in the `CCMSETUP` folder (`C:\Windows\CCMSETUP`) on the client. Although the SCEP client install media is copied to the `CCMSETUP` folder during the ConfigMgr 2012 client install, SCEP won't actually be installed on managed devices until the Endpoint Protection client is enabled and configured in an assigned client settings policy. Also note that the Endpoint Protection client cannot be enabled until the Endpoint Protection site system role is enabled.

You have two choices on how to enable and configure the SCEP client.

- You can make changes to the default client settings policy and enable and configure SCEP there.
- You can create a new, separate settings policy that enables and configures SCEP.

If you wanted every ConfigMgr 2012 client to be configured with the same settings, then you might modify the default client settings, but it's possible that you may want different client setting configurations for different types of devices. For example, you may want any required reboots as a result of the SCEP client install to be suppressed on servers but not be suppressed for desktop devices. So, you may need multiple client settings policies in order to handle certain scenarios.

If you decide to modify the default client settings for the SCEP configuration, you will need to do the following:

1. Open the ConfigMgr 2012 console and choose Administration ➢ Overview ➢ Client Settings.
2. Select the Default Client Settings entry and choose Properties from the ribbon.
3. Select the Endpoint Protection setting and set the required configuration. See Figure 15.2.

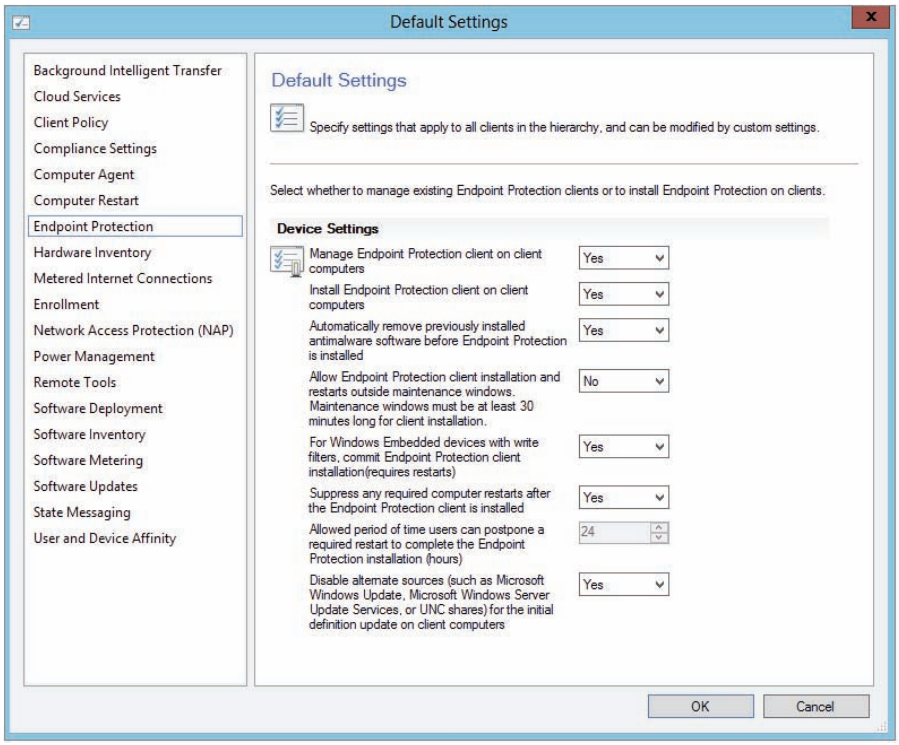


FIGURE 15.2
Endpoint Protection default settings

If you want to create a separate client settings policy for SCEP, follow these steps:

1. Open the ConfigMgr 2012 console and choose Administration ➢ Overview ➢ Client Settings.
2. Click Create Custom Client Device Settings in the ribbon.
3. Give the custom device settings a name and description.
4. Select Endpoint Protection as the custom setting to be enforced on the client devices. See Figure 15.3.
5. Click the Endpoint Protection option on the left side of the window. This will open the Endpoint Protection configuration settings. See Figure 15.4.

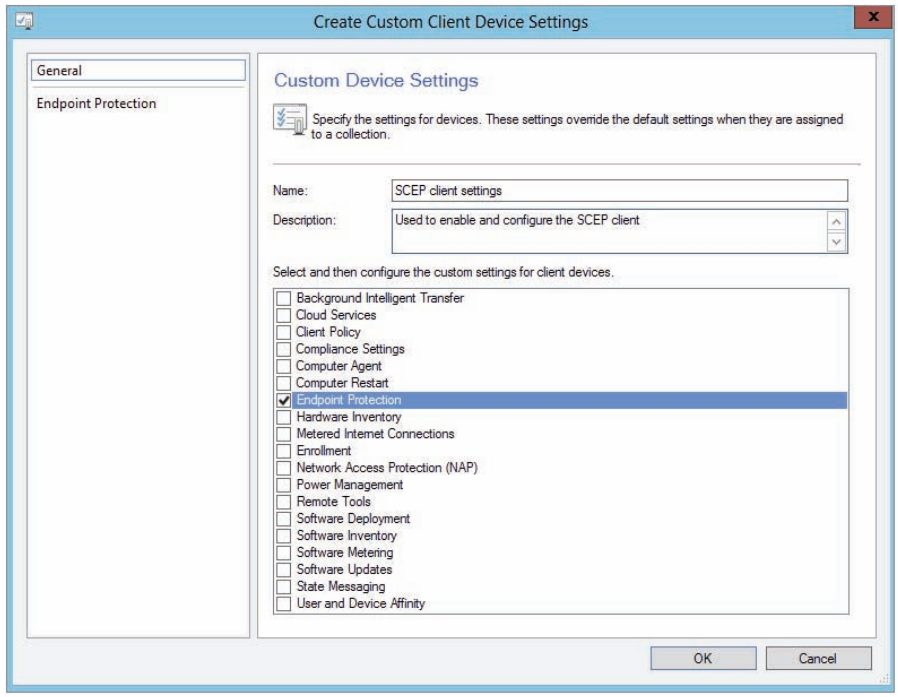


FIGURE 15.3 Selecting the Endpoint Protection custom setting

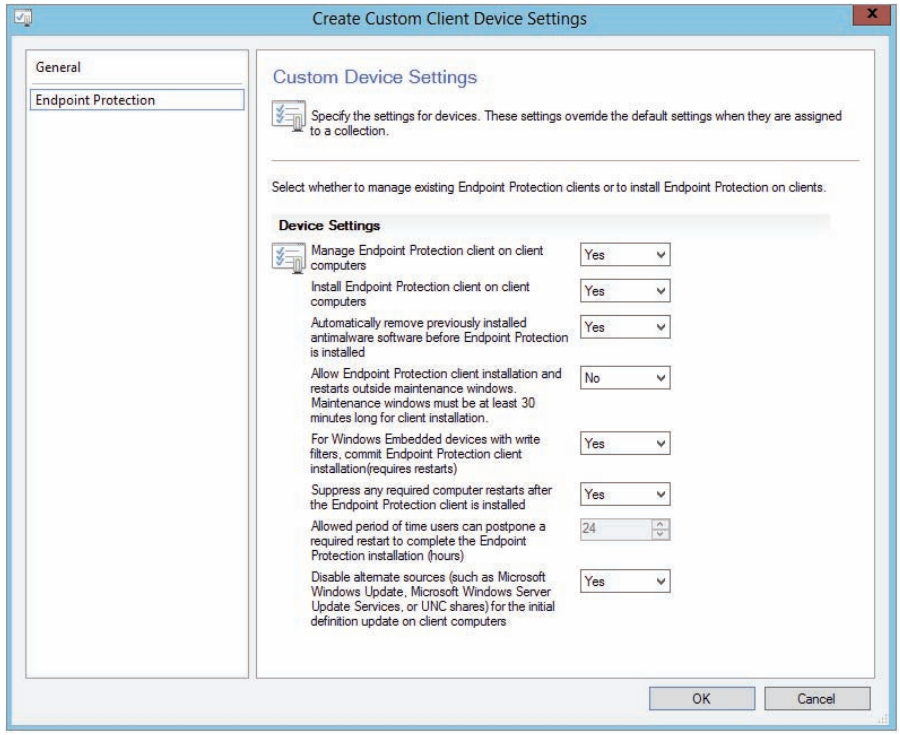


FIGURE 15.4 Configuring Endpoint Protection settings

6. Set the required configuration settings, and click OK.
7. Deploy the new client settings policy to a collection.

After creating the client settings policy for SCEP, don't forget to assign the policy to a collection:

1. Select the policy you created.
2. Choose Deploy from the ribbon.
3. Select the appropriate collection.

Regardless of whether you modify the default client settings or create a new client setting for SCEP, the options that can be configured are the same. As an administrator, you can do the following:

- Define whether the SCEP client should be installed and also if it should be managed.
- Determine if previously installed antimalware software should be automatically removed (see the following list).
- Define if any required reboots after enabling SCEP will be suppressed.
- Disable alternate sources for the initial definition update.

The list of products that can be replaced by SCEP may change somewhat, but the following were the supported titles for removal at the time this book was written:

- Symantec AntiVirus Corporate Edition version 10
- Symantec Endpoint Protection version 11
- Symantec Endpoint Protection Small Business Edition version 12
- McAfee VirusScan Enterprise version 8
- Trend Micro OfficeScan
- Microsoft Forefront Codename Stirling Beta 2
- Microsoft Forefront Codename Stirling Beta 3
- Microsoft Forefront Client Security v1
- Microsoft Security Essentials v1
- Microsoft Security Essentials 2010
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Security Center Online v1

Use this website to obtain an updated list of products that can be removed:

`http://technet.microsoft.com/en-us/library/gg682067.aspx`

If you have an antimalware product installed in the environment that is not on this list, you may need to deploy a removal package for that product. In that scenario, make sure you

coordinate the removal of the old product and the enabling and deployment of the SCEP client and minimize the amount of time that the computer is not protected by antimalware software.

SCEP also supports Mac-based clients as well as Linux/Unix-based clients. The SCEP client installation files for these platforms is available on the Microsoft Volume Licensing website: `www.microsoft.com/Licensing/`.

The supported Macintosh operating systems are as follows:

- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.7 (Lion)
- Mac OS X 10.6 (Snow Leopard)

Note: The SCEP client for the Macintosh operating systems is supported on computers that use the Intel 32-bit and 64-bit chipsets.

The supported Linux/Unix-based operating systems are these:

- RedHat Enterprise Linux (RHEL): versions 6, 5, and 4 (x64 and x86)
- SuSE Linux Enterprise Server (SLES): versions 11, 10, and 9 (x64 and x86)
- CentOS: versions 6 and 5
- Debian: versions 6 and 5
- Ubuntu: versions 12.04 and 10.04
- Oracle Linux: versions 6 and 5

Endpoint Protection Policies

SCEP has two policy types:

Antimalware The antimalware policy is used to define the antimalware settings that will be applied to the endpoint client.

Windows Firewall The Windows Firewall policy can be used to control the configuration of Windows Firewall on managed computers.

Both types of Endpoint Protection policies can be created and modified in the ConfigMgr 2012 console.

Antimalware Policy

ConfigMgr 2012 includes a default antimalware policy (Default Client Malware Policy) that can be modified. However, you should understand that changes made to that policy will be applied to all managed computers in the environment. Instead, the ConfigMgr administrator may decide to create a custom policy (or policies), and those policy settings would override the default client policy.

The following configuration changes can be made in the antimalware policy:

Scheduled Scans This option defines various information about the antimalware scan, including when the scan should occur, when the definition files should be updated, and if CPU usage should be limited. See Figure 15.5.

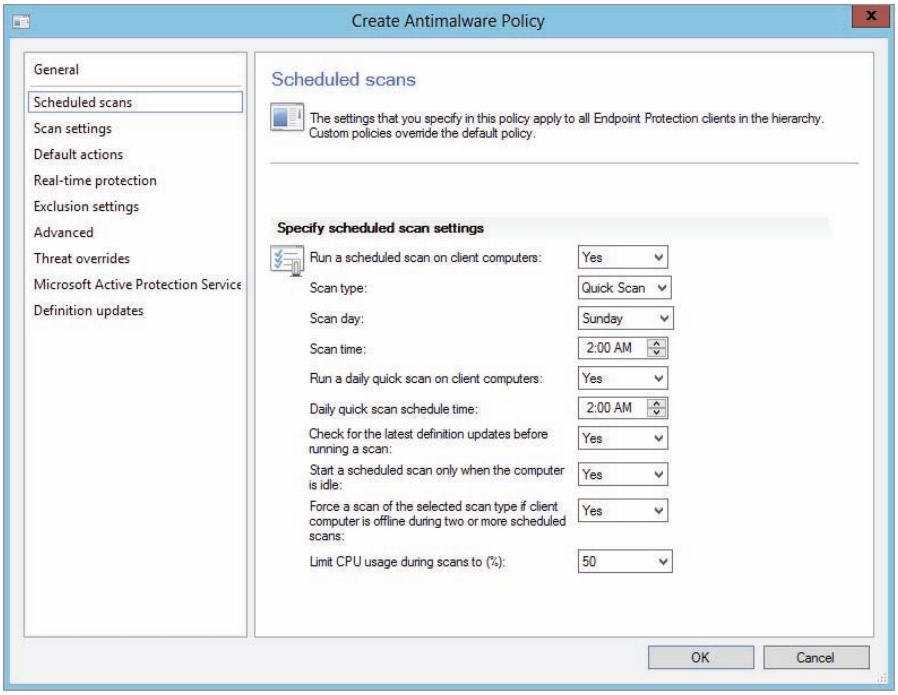


FIGURE 15.5
Configuring the Scheduled Scans settings

QUICK SCAN OR FULL SCAN?

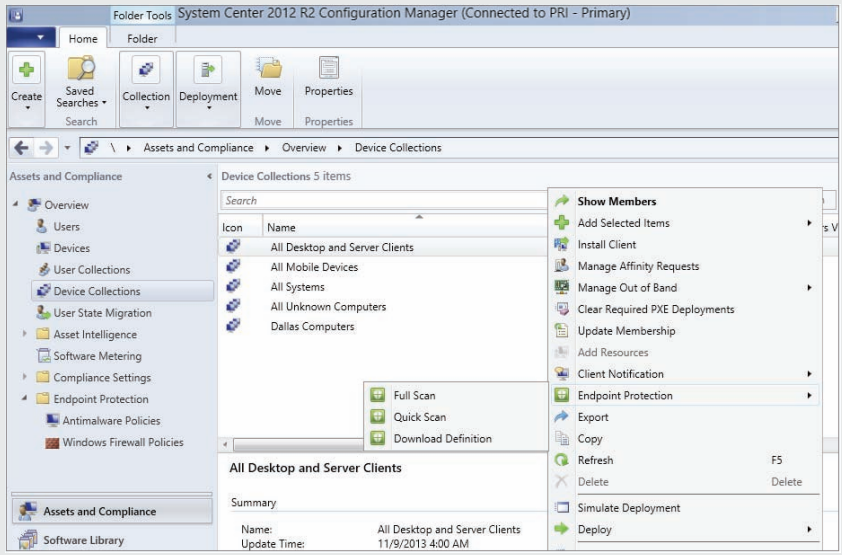
The Scheduled Scans option allows you to configure when quick and full scans occur. But what is the difference between a quick scan and a full scan?

A quick scan does a check on locations where malware likes to hide in memory and on the hard drive. A quick scan should take only a few minutes, and performing the quick scan daily is a good practice.

A full scan checks all of the files on the hard disk and also checks memory and all programs that are currently active. This scan is more intensive and uses more resources on the computer, so performance on the computer may be impacted somewhat. This scan should typically be performed weekly and at a time when the computer will be on but not in use.

In the event of an active malware outbreak, you can trigger a quick or a full scan or a definition file download from the ConfigMgr 2012 console. The specified action will utilize the client communication channel and should take place immediately if the client is accessible. To trigger the scan or definition file download action, follow these steps:

1. Select Assets And Compliance ➢ Overview ➢ Device Collections.
2. Right-click the appropriate collection.
3. Select Endpoint Protection, and choose the appropriate action (Full Scan, Quick Scan, or Download Definition), as shown in the following illustration.



This will initiate an antimalware scan or definition download against the member computers of the collection.

Scan Settings This option defines what types of items should be scanned and also defines whether the end user can change the scan settings (Figure 15.6).

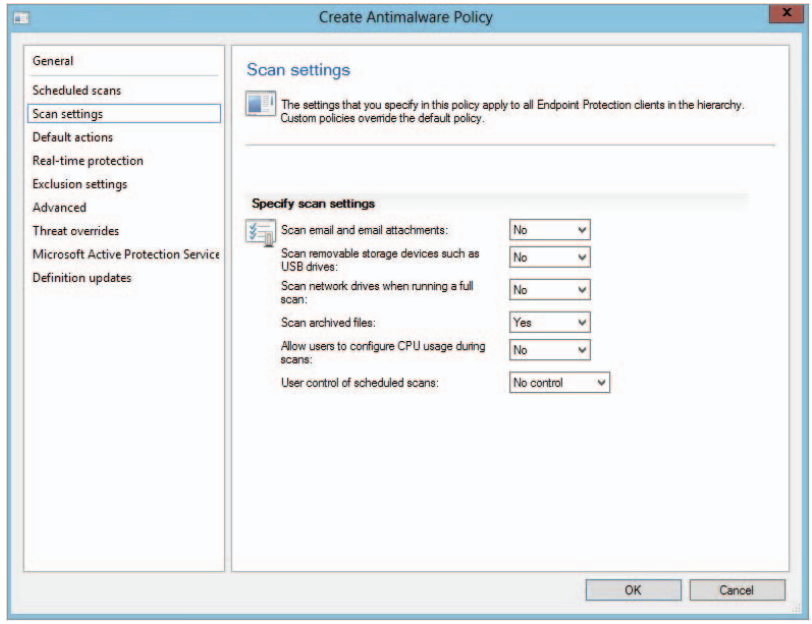


FIGURE 15.6 Configuring the Scan Settings

Default Actions This option defines the action that will be taken on threats based on their classification (Figure 15.7).

Real-Time Protection This option defines the configuration of real-time protection and scanning (Figure 15.8).

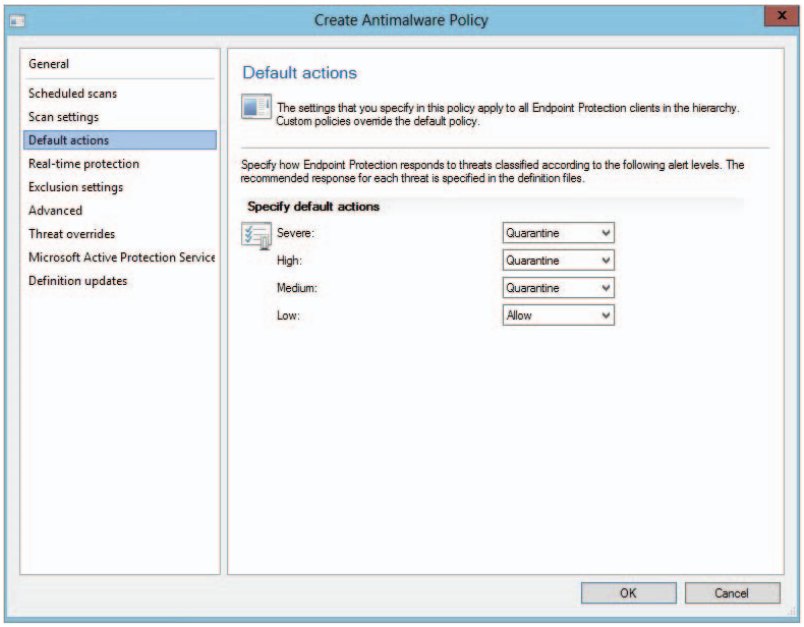


FIGURE 15.7 Configuring the Default Actions settings

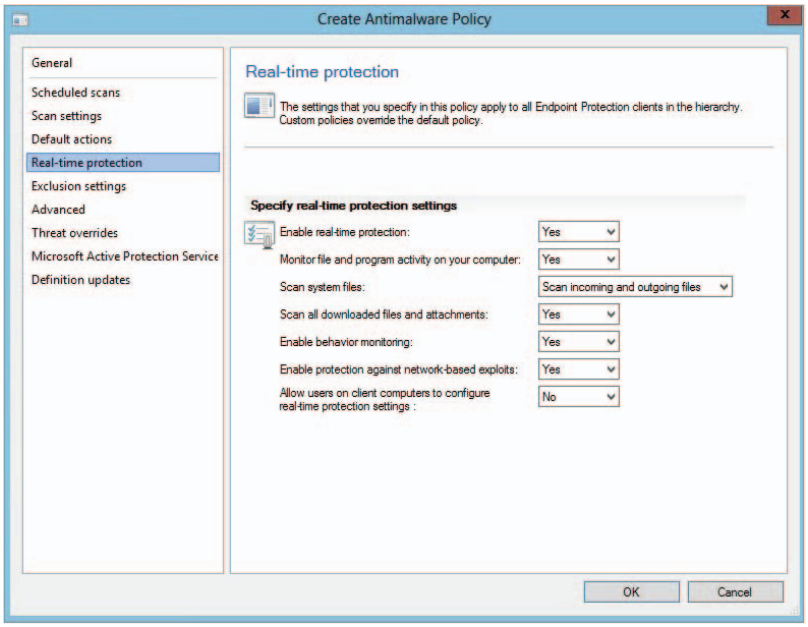


FIGURE 15.8 Configuring the Real-Time Protection settings

Exclusion Settings This option defines any files, folders, file types, or processes that should be excluded from malware scanning (Figure 15.9). Note that excluding items may increase the risk of malware not being detected on a computer.

Advanced This option provides the ability to customize advanced settings, including interaction with users, how long quarantined files should be retained, and so on (Figure 15.10).

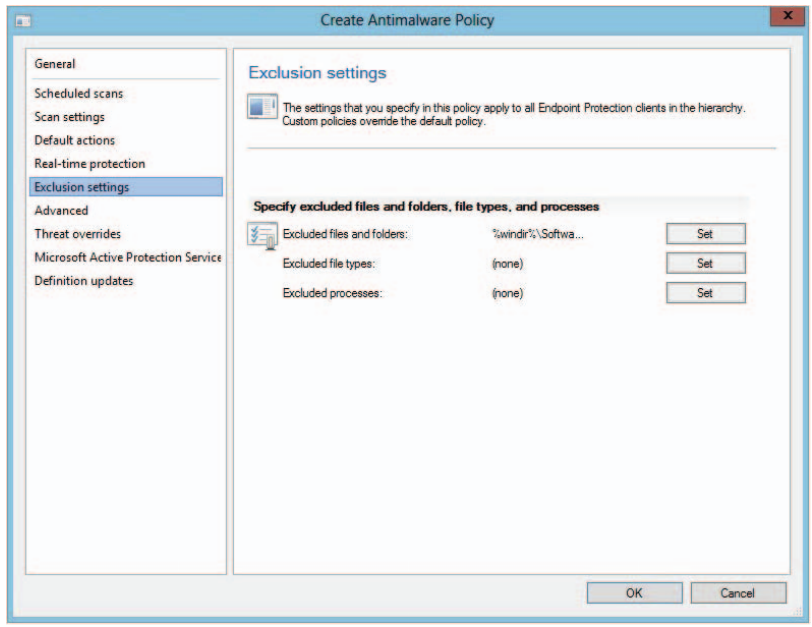


Figure 15.9 Configuring the Exclusion Settings

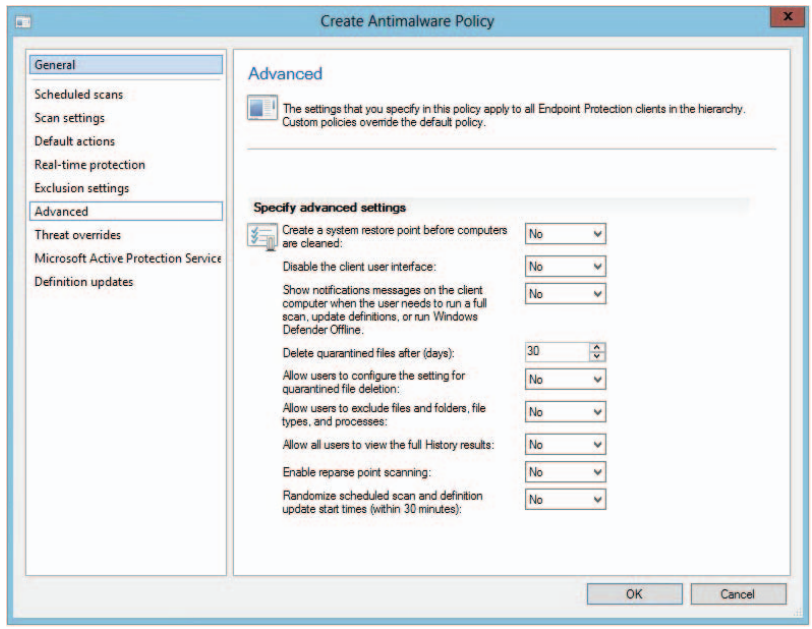


Figure 15.10 Configuring the Advanced settings

Threat Overrides This option allows you to add threat names to the threat list (Figure 15.11).

Microsoft Active Protection Service This option allows you to configure MAPS (Figure 15.12).

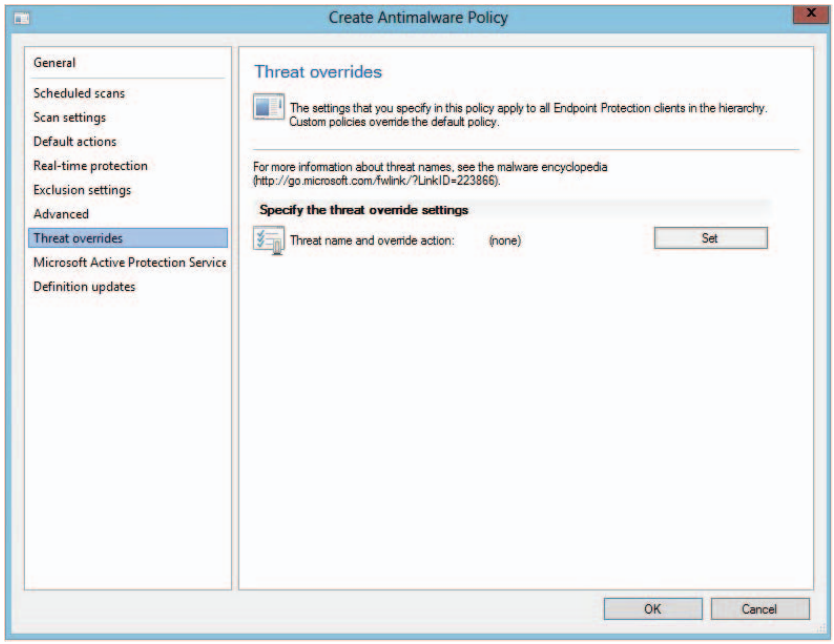


FIGURE 15.11 Configuring the Threat Overrides settings

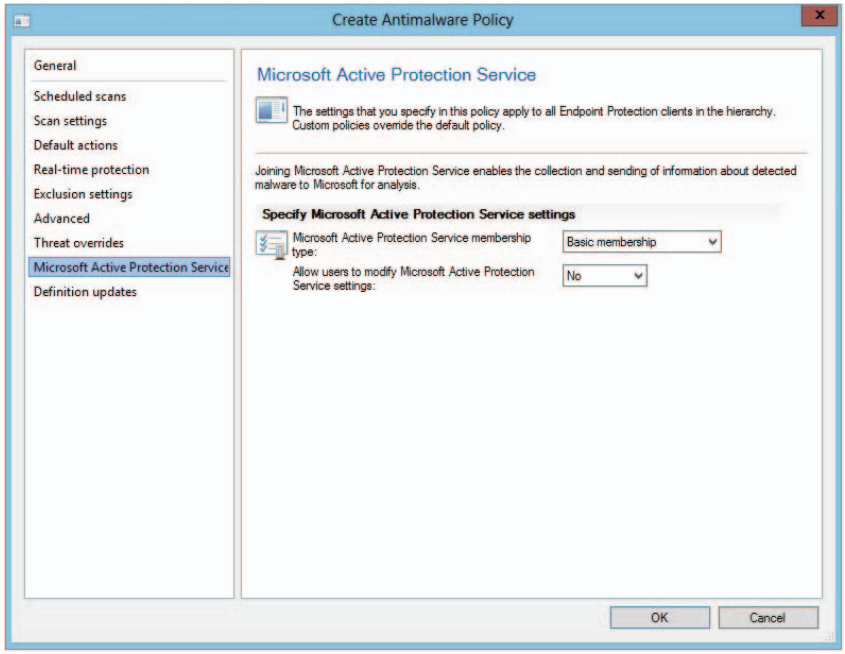


FIGURE 15.12 Configuring the MAPS settings

Definition Updates This option allows you to configure how Endpoint Protection clients will receive definition updates (Figure 15.13).

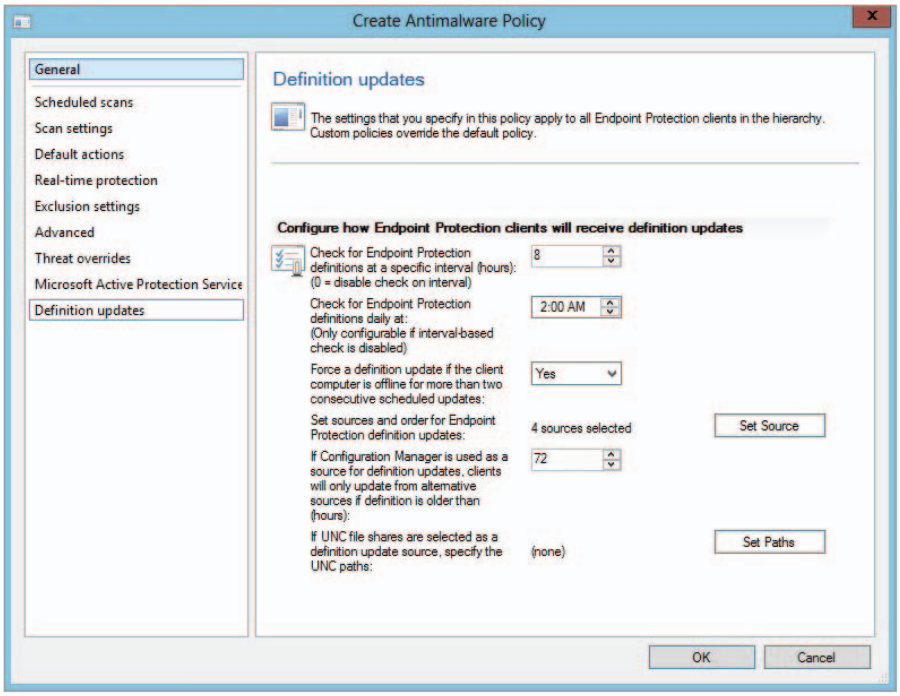


FIGURE 15.13
Configuring the Definition Updates settings

ConfigMgr 2012 includes a number of predefined antimalware policy templates for several Microsoft products, including ConfigMgr 2007 and 2012, SQL 2005 and 2008, Exchange Server, and Windows. The complete list of policies that are provided with ConfigMgr 2012 can be viewed in the following folder on the ConfigMgr 2012 site server:

```
..\Microsoft Configuration Manager\AdminConsole\XmlStorage\EPTemplates
```

These policies apply settings that are optimized for a particular product or feature and can easily be imported and used in the environment. You can also import antimalware policies that were created in FEP 2010.

In ConfigMgr 2012 you can also merge policies by taking a default policy and merging it with another policy. This scenario may be useful if you want to use the default client policy but apply some specific file or folder exclusions that were included in one of the policies that was imported.

Windows Firewall Policy

The SCEP feature of ConfigMgr 2012 can also be used to manage the Windows Firewall policies for managed computers. ConfigMgr 2012 does not include a default Windows Firewall policy,

and there is no ability to import or export a policy, but you can easily create a new policy in the ConfigMgr 2012 console.

As you can see in Figure 15.14, the Windows Firewall policy configuration is straightforward. You can create a new Windows Firewall policy in the ConfigMgr 2012 console and configure the policy to enable/disable the firewall, to block incoming connections, and also to define user communication. Once you have configured the policy, you can then deploy it to a collection.

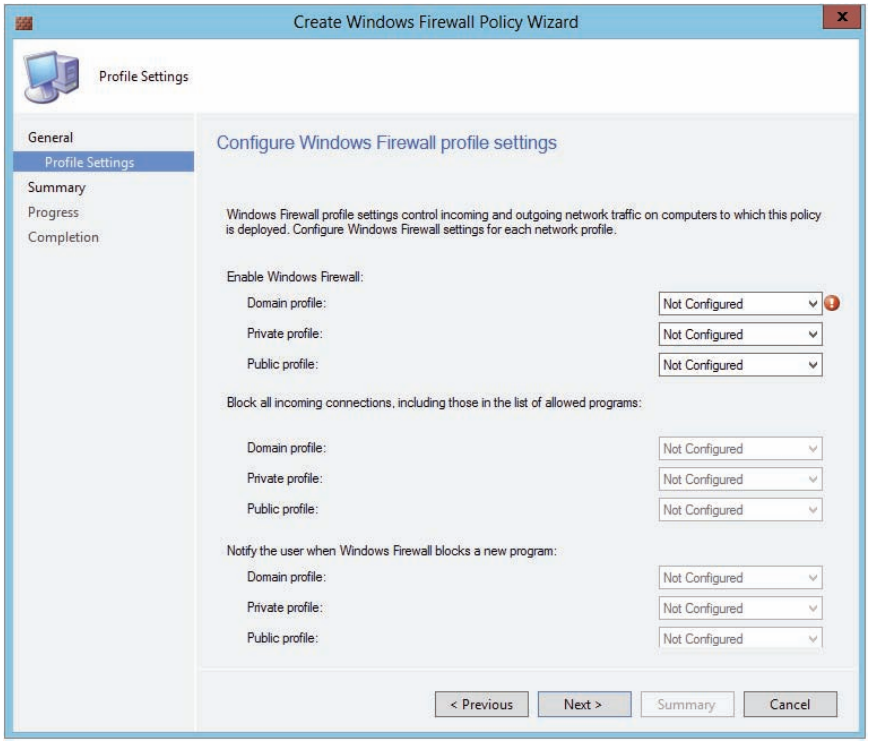


FIGURE 15.14
Configuring Windows Firewall policy

You may notice that there are three profile types: domain, public, and private. These profiles are related to the network that the user or computer is connected to.

Domain The domain profile will be applied if the connection is authenticated to a domain controller for the domain of which the user or computer is a member. By default, all other network connections are initially classified as public networks, and Windows asks the user to identify the network as either public or private.

Public The public profile is intended for use in public locations (such as airports and coffee shops).

Private The private network location is typically intended for use in a home or office.

Assigning Policy

The Default Client Malware Policy is automatically applied to all of the computers managed by ConfigMgr 2012. If you create a custom policy and assign it to a collection, the settings in the custom policy will override the settings that are defined in the default policy.

Use the following steps to assign a custom antimalware policy to a collection:

1. Open the ConfigMgr 2012 console and choose Assets And Compliance ➢ Overview ➢ Endpoint Protection ➢ Antimalware Policies.
2. Select the custom policy and choose Deploy from the ribbon.
3. Select the collection, and click OK.

The next time the ConfigMgr 2012 clients in the targeted collection retrieve policy (every 60 minutes by default), they will apply the SCEP client settings that were established in the policy. If two custom policies have different values configured for the same settings, the policy with the highest Order value will be applied. You can adjust the order in the ConfigMgr console by right-clicking the custom policy and selecting Increase Priority or Decrease Priority. See Figure 15.15.

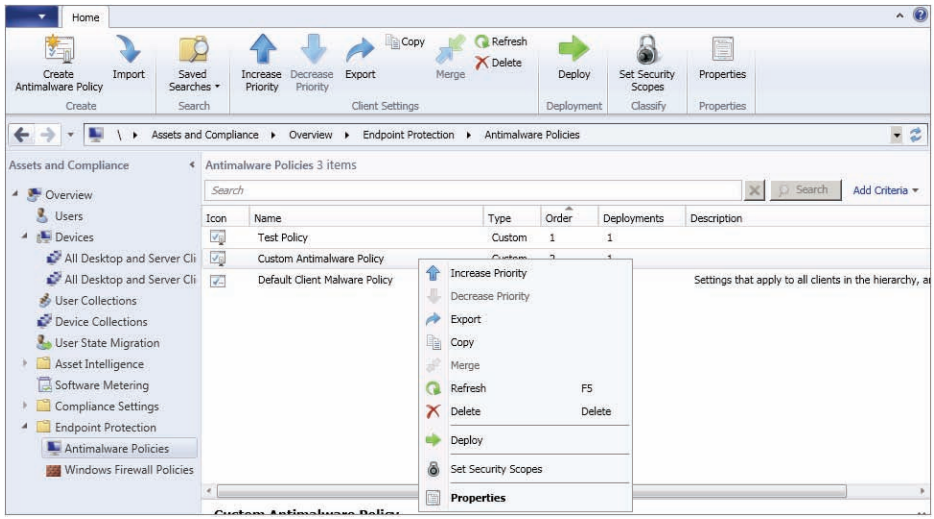


FIGURE 15.15 Increasing policy priority

DEFAULT ORDER VALUE

The order for the Default Client Malware Policy has a default value of 10,000 and cannot be changed.

Definition Files

As discussed in Chapter 9, "Software Updates," ConfigMgr 2012 provides the ability to automatically download and deploy security updates to managed computers using a feature called Automatic Deployment Rules (ADR). These rules can be used for monthly security

updates (Patch Tuesday, for example), and they can also be used for SCEP definition file updates. The SCEP definition files are updated several times a day, and you need an automated solution like ADR to handle the download and deployment of the updated files as they become available. For more information on how to create automatic deployment rules, refer to the software updates chapter in this book.

Once the automatic deployment rules for SCEP have been configured, you may want to verify that the automatic deployment rules are working properly for the SCEP definition updates. The following process will ensure that the clients have the latest definition files.

The first question is what is the latest version of the Endpoint Protection definition files? Checking the Microsoft Malware Protection Center website

```
http://www.microsoft.com/security/portal/Definitions/HowToForeFront.aspx
```

is one quick method to provide that answer.

As you can see in Figure 15.16, the latest Forefront definition update that was available at the time this image was captured is 1.161.1740.0. So you now know how to tell which version of the definition file the environment should be using.

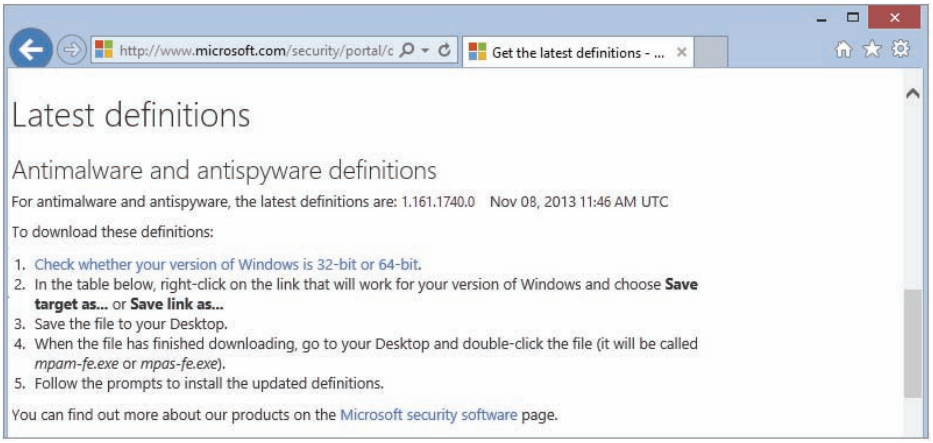


FIGURE 15.16 Obtaining the definition update version

If you open the ConfigMgr 2012 console and choose Software Library ➢ Overview ➢ Software Updates ➢ All Software Updates, you can view the list of software updates in the catalog. If you search for "endpoint," you can look for software updates that have a matching title and focus on the SCEP definition files.

Expect to see several definition files listed, but only one should typically be current and active (the green arrow indicates the current definition file). As you can see in Figure 15.17, the version of that file is 1.161.1740.0, so all of your clients should be using that version of the definition file. Note that superseded updates have yellow arrows and the expired definition files have a black *X*.

You now know that the endpoint clients should be using version 1.161.1740.0 of the definition file. If you open the SCEP client on a managed workstation, you can check the definition file that is currently being used by the client. See Figure 15.18.

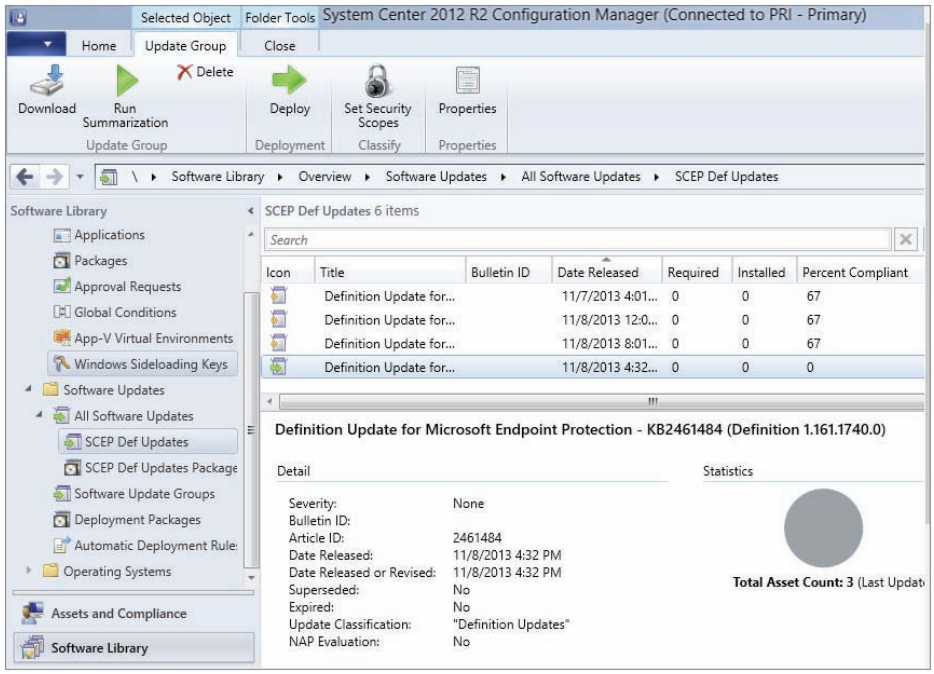


FIGURE 15.17
Definition update status

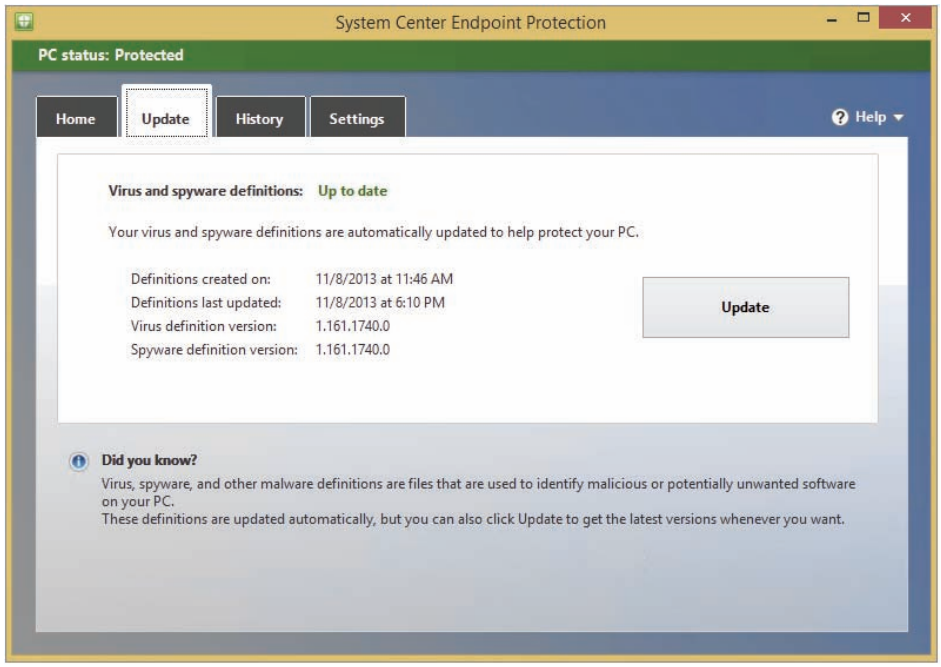


FIGURE 15.18
Verifying SCEP client definition version

As you can see, this client is using the correct version of the definition file. If the definition file is an older version, it's possible that the client hasn't triggered the process yet to get the latest definition file. You could click Update and force the client to obtain the latest file. If the client still does not have the latest definition file, then you may need to troubleshoot the issue further and determine why the client is unable to retrieve the updated content.

Alerts

The ability to create alerts is new in ConfigMgr 2012. Alerts can be used to notify a ConfigMgr administrative user when specific events (such as a malware outbreak) have occurred in the environment. The administrator can view alerts in the ConfigMgr 2012 console, in reports, and also via email subscriptions. The ability to display alerts in the console or via email is especially important for SCEP-related events because it allows the administrator to quickly become aware of a malware event.

ConfigMgr 2012 Alerts vs. SCOM Alerts

The alert feature in ConfigMgr 2012 should not be confused with the alerting that is provided in the System Center Operations Manager product.

SCEP alerts are configured in the device collection properties. You cannot configure user collections for alerts. ConfigMgr 2012 has alerts for various issues and conditions and includes four alerts related specifically to malware:

Malware Detection An alert is generated if a managed computer in the specified collection has malware.

Malware Outbreak An alert is generated when a certain percentage of managed computers in the specified collection have malware detected.

Repeated Malware Detection An alert is generated if specific malware is detected more than a certain number of times over a certain number of hours in a specified collection.

Multiple Malware Detection An alert is generated if more than a specified number of malware types are detected over a given period for a specified collection.

In order to receive alerts you must enable a device collection to send alerts. The following is the process:

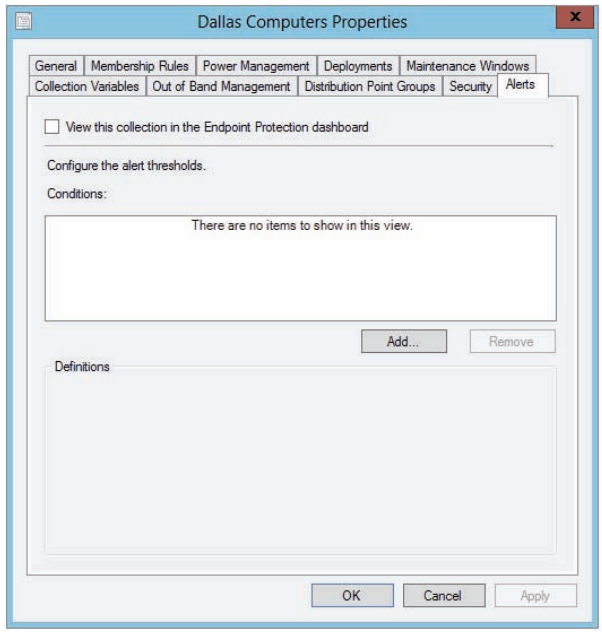
1. In the ConfigMgr 2012 console, select the device collection that should be configured to send alerts, and select Properties from the ribbon.

   In this example we will select a collection named Dallas Computers.

2. In the collection properties window, select the Alerts tab. See Figure 15.19.

3. Enable the View This Collection In The Endpoint Protection Dashboard option, and click Add to specify alert thresholds.

Figure 15.19
Alerts tab in the collection properties



Enabling a Collection

Until you enable a collection to be viewed, the System Center 2012 Endpoint Protection Status node in the Monitoring workspace of the ConfigMgr 2012 console will be blank, and a message will appear: "No collections have been configured to display in Endpoint Protection status."

When you click Add to specify alert thresholds, the Add New Collection Alerts window will appear, and all of the items will be unchecked by default. The needs of the administrative users may vary, but we will assume for this scenario that all of the alert conditions are needed in the environment.

4. Select each option and click OK (Figure 15.20).
5. If you want to customize the thresholds, you can, but for now use the default settings and click OK (Figure 15.21).

At this point you have configured the devices in a collection to generate alerts if the alert conditions are met. Those alerts can be viewed in the console, viewed in reports, and also sent via email subscriptions.

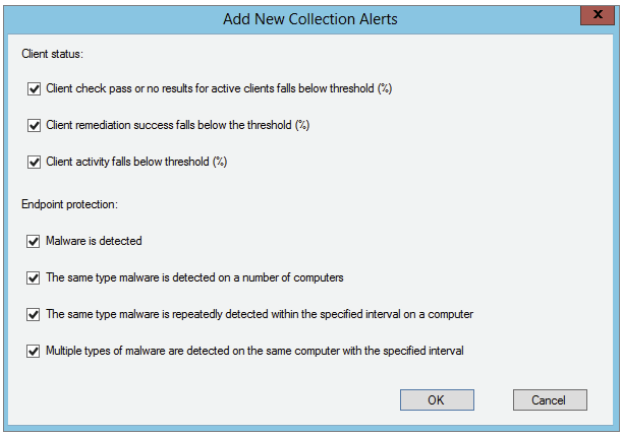


FIGURE 15.20
Enabling collection alerts

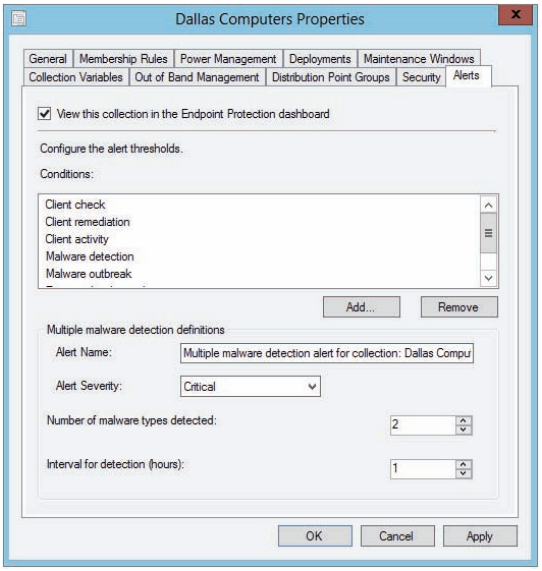
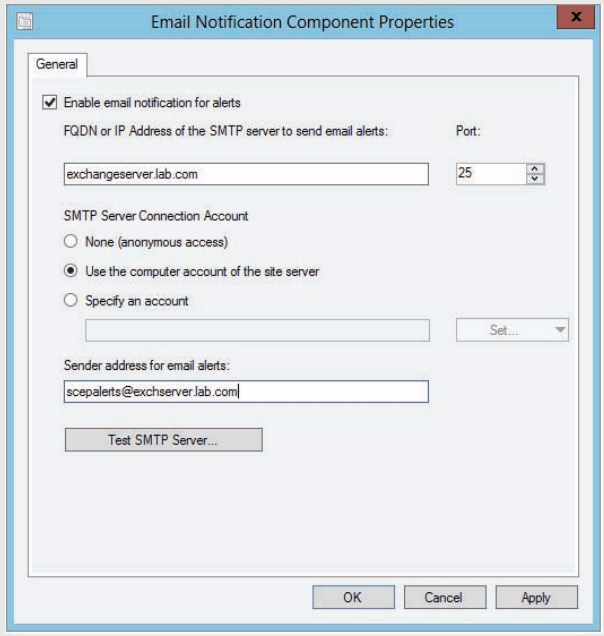


FIGURE 15.21
Setting alert thresholds

CONFIGMGR CAN SEND YOU EMAIL

In ConfigMgr 2012 you can configure an SMTP server that will be used to email Endpoint Protection alerts to administrative users. Follow these steps:

1. In the ConfigMgr 2012 console, choose Administration ➢ Overview ➢ Site Configuration ➢ Sites.
2. Select the CAS (or standalone primary site server) and click Settings ➢ Configure Site Components ➢ Email Notification.
3. Enable the email notification option, as shown in the following illustration, enter the required email settings for your environment, and click Apply.



You also have the option to test the SMTP server and verify that the configuration is set properly.

4. Configure alert email subscriptions in the Monitoring workspace by choosing Monitoring ➢ Overview ➢ Alerts ➢ Subscriptions and select Create Subscription in the ribbon.

Reporting

ConfigMgr 2012 has several reports related to the Endpoint Protection products. There are currently six reports in the Endpoint Protection category:

Antimalware Activity Report This report shows an overview of antimalware activity and is shown in Figure 15.22.

Antimalware Overall Status And History This report shows an overall status of antimalware activity over a specified period.

Computer Malware Details This report shows the endpoint client status and antimalware activity.

Infected Computers This report shows a list of computers with a particular threat detected.

Top Users By Threats This report lists the users with the highest number of detected threats.

User Threat List This report shows the list of threats found under a particular user account.

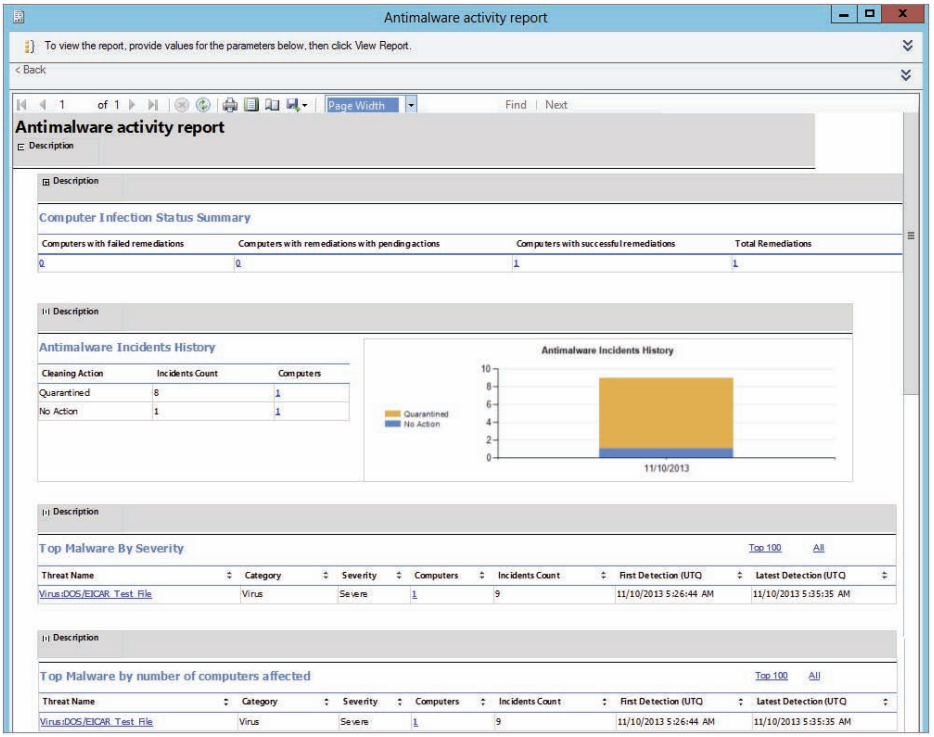


FIGURE 15.22
Antimalware Activity Report

Client Notifications

Many activities in Configuration Manager are pull-based and use polling intervals and scheduled intervals to define when processes take place. This is acceptable for many features in Configuration Manager, but in the case of an outbreak of malware in an environment, an administrator may need to take immediate action on the managed clients and not wait for a policy cycle to occur. Configuration Manager accomplishes this expedited communication process by creating a client notification channel between the site server and the managed clients. This "fast" channel is used for all endpoint-related activities as well as the computer policy download client action. This channel is a push-based communication process and allows a Configuration Manager administrator to take immediate action against clients, like forcing clients to perform a scan to look for malware. The client notification channel is supported only on Windows devices.

The client notification process consists of several parts. The Notification Manager component exists on the Configuration Manager site server and the notification server exists on the management points. The notification agent is part of the Configuration Manager client. The notification agent on the client initiates a persistent connection with the notification server and will attempt to use TCP mode first and then fallback to HTTP if TCP mode fails. Once the connection is established, the notification agent will send a keep-alive message every 15 minutes to maintain the connection with the notification server. The default TCP port is 10123.

The following are the related Configuration Manager logs for the client notification channel components:

Notification Manager: `..\Microsoft Configuration Manager\Logs\bgbmgr.log`
Notification Server: `..\Microsoft Configuration Manager\Logs\BgbServer.log`
Notification Agent: `C:\Windows\ccm\logs\CcmNotificationAgent.log`

For example, if you use the Configuration Manager console to trigger a quick malware scan against a client computer, you can monitor the client communication channel request via the `CcmNotificationAgent.log` on the client and the status of the endpoint scan via the `EndpointProtectionAgent.log`. See Figure 15.23.

We will use the remainder of this chapter to work through a real-world scenario and show SCEP in action.

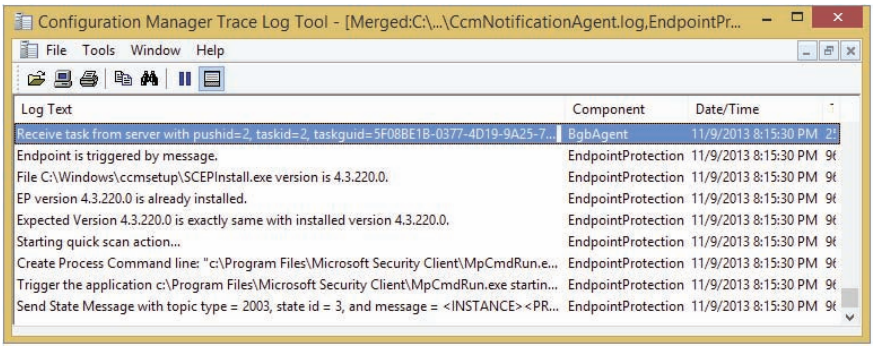


FIGURE 15.23 Notification Agent log and Endpoint Protection log

Real World Scenario

LET'S DEPLOY SOME MALWARE!

You are the ConfigMgr 2012 administrator at a company, and you have been telling your fellow IT department personnel about all of the great features that have been added to the ConfigMgr product. You are especially excited about the Endpoint Protection feature and the security against malware that it provides.

Your manager has asked you to demonstrate to the team how the SCEP feature works. You decide it would be a great demo to actually deploy malware to the environment and have ConfigMgr 2012 identify the outbreak and remediate it. Seems a bit risky, right? And where do you get a virus so that you can prove SCEP works? Download some questionable files from the Internet or click on that email attachment from an unknown person? Not likely. It would be much safer to use a test virus, a piece of software that *looks* like malware but doesn't actually cause any damage.

One option is to use the antimalware test file that was created by the IT security research organization called EICAR (you can read more about them at `www.eicar.org`). The EICAR test file that they provide on their website looks like a virus or malware to antimalware software, but it is completely safe and benign. The test file simulates a malware attack but does not harm the computer in any way. However, just to be safe, you decide to perform this demo in your ConfigMgr 2012 test environment that is separated from the production network.

Using the EICAR antimalware test file, in a *test* ConfigMgr 2012 environment that is *not* connected to the production network, you can safely simulate the occurrence of a malware event on a managed computer without actually damaging the computer or causing a malware outbreak panic.

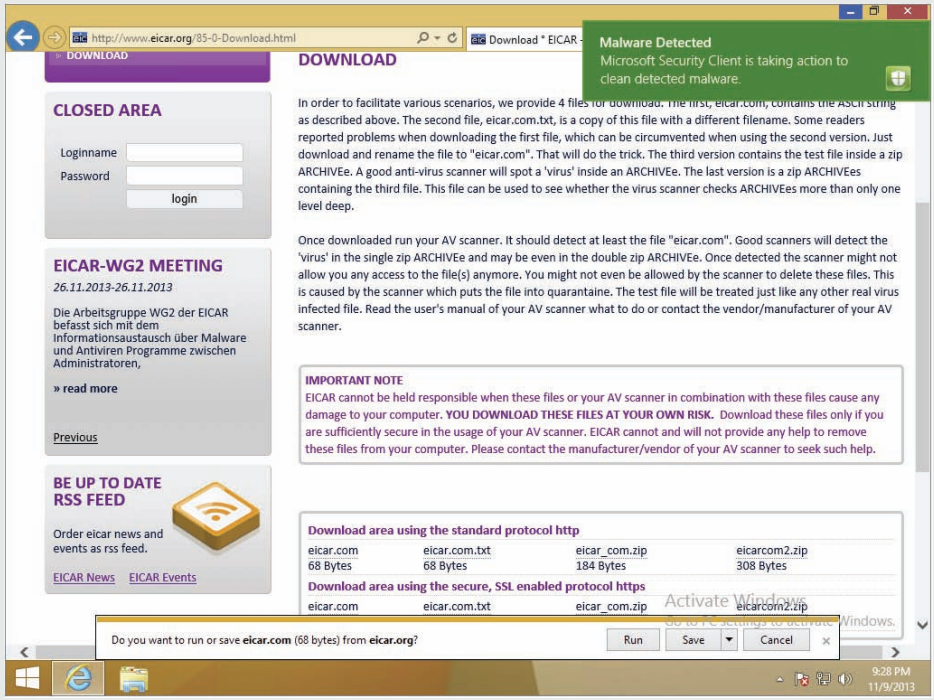
Note: Before using this tool, visit the EICAR website and make sure you read through all of the documentation and disclaimers for the use of the tool.

Run the Test!

You are now ready to run the demo for your team.

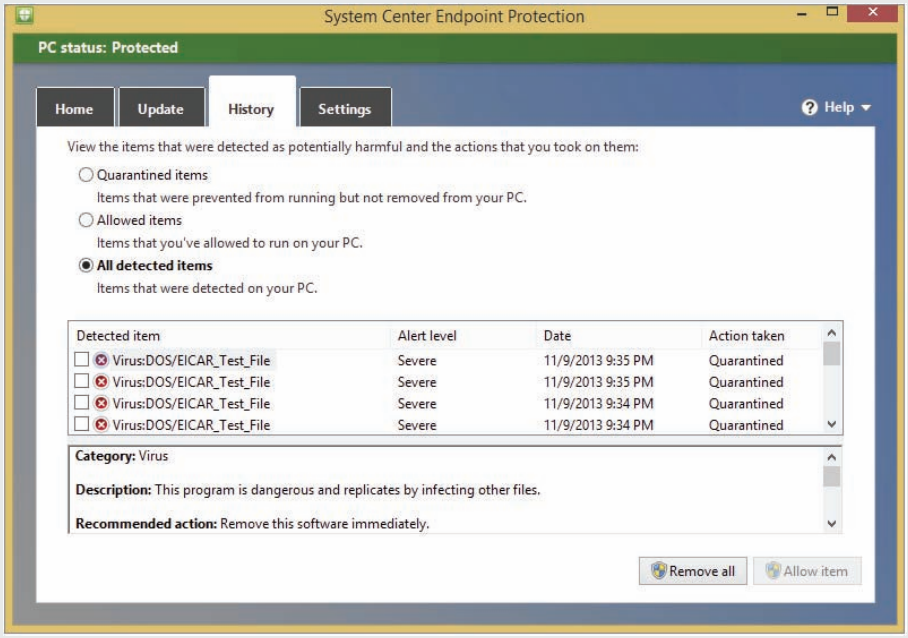
1. Log onto the Windows computer that will become your "infected" workstation, launch the EICAR malware test file, and then monitor the results.

   First, you see by the green status window that SCEP on the Windows computer detected malware and is taking action to remove it.



The antimalware policy for this environment was configured to quarantine threats, but you could also configure it to automatically remove them.

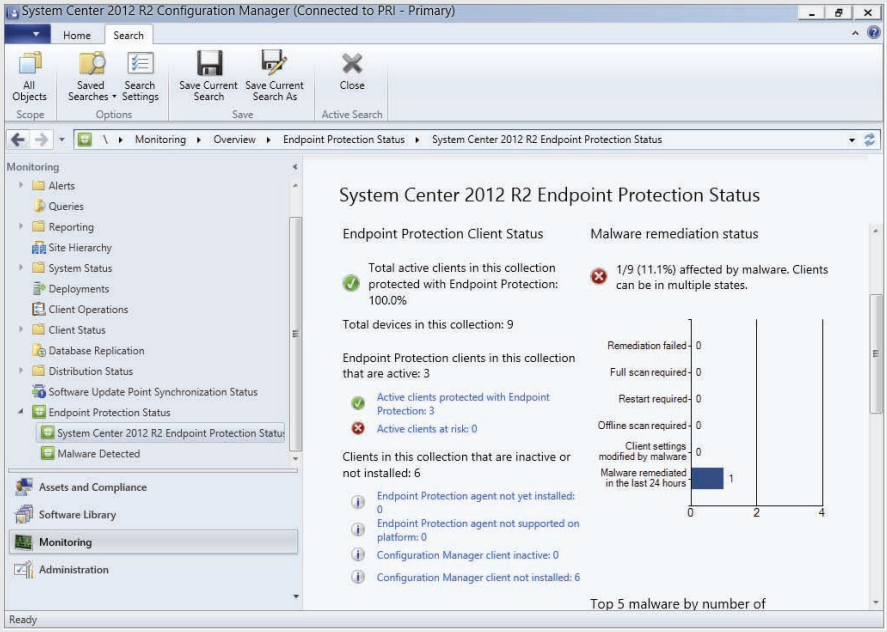
2. Look at the SCEP client on the computer, choose the History tab, and see the malware activity. You can view the name of the detected malware item, the alert level, the date and time the event occurred, and the action that was taken.

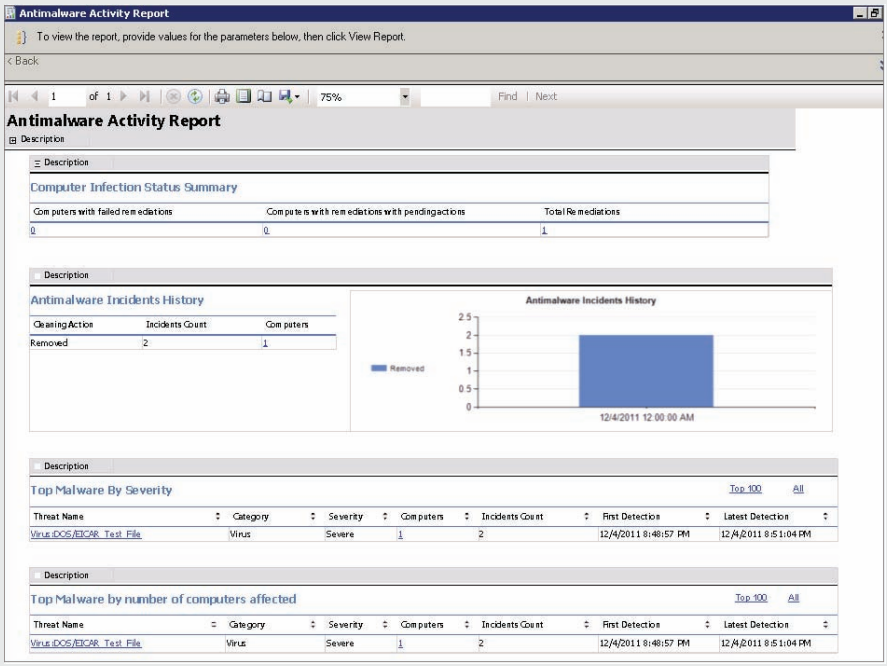


But What Happened on the Site Server?

You saw SCEP on the Windows computer flag the EICAR test file as malware and immediately quarantine the malware. But what would you see at the site server level? How would the built-in monitoring make you aware of the issue? Follow these steps to find out:

1. Open System Center 2012 Endpoint Protection Status in the ConfigMgr 2012 console (Monitoring ➢ Overview ➢ Endpoint Protection Status ➢ System Center 2012 R2 Endpoint Protection Status).
2. Select the collection (All Systems in this case) to see the overall status for the environment, including the number and percentage of clients that were affected by malware (one computer in this test). You can also view the top 5 malware by number of computers and the status of the definition files on managed computers in this window.
3. You could open the Alerts section of the Monitoring workspace to view the alerts that were generated as a result of the EICAR malware test being executed on the client, and if you have configured email subscriptions, you would have received those alerts as emails.
4. You can also use the endpoint reports to view the status of the environment. Select the Antimalware Activity Report to view the overall status. You can clearly see the total number of remediations, the number of antimalware incidents, and so on.


System Center 2012 R2 Configuration Manager (Connected to PRI - Primary)
Home
Search
All Objects
Saved Searches
Search Settings
Save Current Search
Save Current Search As
Close
Scope
Options
Save
Active Search
Monitoring ▸ Overview ▸ Endpoint Protection Status ▸ System Center 2012 R2 Endpoint Protection Status
Monitoring
Alerts
Queries
Reporting
Site Hierarchy
System Status
Deployments
Client Operations
Client Status
Database Replication
Distribution Status
Software Update Point Synchronization Status
Endpoint Protection Status
System Center 2012 R2 Endpoint Protection Status
Malware Detected
Assets and Compliance
Software Library
Monitoring
Administration
System Center 2012 R2 Endpoint Protection Status
Endpoint Protection Client Status
Total active clients in this collection protected with Endpoint Protection: 100.0%
Total devices in this collection: 9
Endpoint Protection clients in this collection that are active: 3
Active clients protected with Endpoint Protection: 3
Active clients at risk: 0
Clients in this collection that are inactive or not installed: 6
Endpoint Protection agent not yet installed: 0
Endpoint Protection agent not supported on platform: 0
Configuration Manager client inactive: 0
Configuration Manager client not installed: 6
Malware remediation status
1/9 (11.1%) affected by malware. Clients can be in multiple states.
Remediation failed 0
Full scan required 0
Restart required 0
Offline scan required 0
Client settings modified by malware 0
Malware remediated in the last 24 hours 1
0 2 4
Top 5 malware by number of
Ready


Antimalware Activity Report
To view the report, provide values for the parameters below, then click View Report.
Back
1 of 1
75%
Find | Next
Antimalware Activity Report
Description
Computer Infection Status Summary
Computers with failed remediations
Computers with remediations with pending actions
Total Remediations
0
0
1
Antimalware Incidents History
Cleaning Action
Incidents Count
Computers
Removed
2
1
Antimalware Incidents History
Removed
2.5
2
1.5
1
0.5
0
12/4/2011 12:00:00 AM
Top Malware By Severity
Top 100
All
Threat Name
Category
Severity
Computers
Incidents Count
First Detection
Latest Detection
Virus:DOS/EICAR_Test_File
Virus
Severe
1
2
12/4/2011 8:48:57 PM
12/4/2011 8:51:04 PM
Top Malware by number of computers affected
Top 100
All
Threat Name
Category
Severity
Computers
Incidents Count
First Detection
Latest Detection
Virus:DOS/EICAR_Test_File
Virus
Severe
1
2
12/4/2011 8:48:57 PM
12/4/2011 8:51:04 PM

Summary

You were able to demonstrate the effectiveness of the System Center 2012 Endpoint Protection feature of ConfigMgr 2012 to your peers, and they gave you a standing ovation — and bought you lunch.

The Bottom Line

Differentiate between FEP and SCEP. There are several differences between FEP and SCEP, including the architecture and the deployment process.

Master It Where does SCEP store its data?

Deploy and configure the System Center 2012 Endpoint Protection site system and client. The three main components of enabling SCEP are as follows:

- Install and configure the Endpoint Protection site system.
- Enable and configure the SCEP client.
- Configure the antimalware policies.

Master It Do you need to create a package or application to deploy the SCEP client?

Create and assign an SCEP policy. SCEP has two types of policy:

- Antimalware
- Windows Firewall

The antimalware policy is used to define the antimalware settings, while the Windows Firewall policy can be used to control the configuration of Windows Firewall on managed computers. Both types of Endpoint Protection policies are created and modified in the ConfigMgr 2012 console.

Master It If you modify the default client antimalware policy and also create a custom antimalware policy with different values for the settings and apply it to a collection, which settings will be applied?



Chapter 16

Mobile Device Management

The power of the mobile device as a computing platform has grown significantly in recent years. The number of mobile devices is increasing all the time. The devices are a favorite among the user community and are definitely here to stay. Having a mechanism to manage these devices effectively is crucial to IT because users demand to bring their own devices.

These devices are now a significant part of the computing landscape and are only accelerating in relevance. As a result, organizations of all sizes are tasked with finding the best way to handle these devices, allowing users the flexibility inherent with these devices while balancing the needs of corporate security and management when these devices are used in an enterprise setting.

A further challenge is the sheer number of device types and operating systems in use, including devices running the Windows Phone or Windows Mobile 8 operating systems, devices from Apple such as the iPhone or iPad, devices running the Android or BlackBerry platforms, and others. Each device type and operating system allows for different management capabilities—and these capabilities will continue to evolve over time. Being able to manage these devices consistently, regardless of the type of device, is important for organizations and is exactly what Configuration Manager 2012 is designed to do. With the extension of Configuration Manager 2012 R2 to the cloud service Windows Intune, Configuration Manager has become a fully mature mobile device management solution.

This chapter will detail the mobile device management options available in Configuration Manager 2012.

In this chapter, you will learn to

- Detail the differences between lite and depth management
- Understand how to configure mobile device management
- Understand the depth-management enrollment process

What's New in Mobile Device Management

The mobile devices world has changed at an amazing pace since the last full release of Configuration Manager, version 2007. A variety of device and operating system manufacturers are in the market, and the number of users with mobile devices has grown significantly. Mobile devices have become center stage for many users, and such devices are often the single computing device where users spend the bulk of their time. These devices often blur the lines between the individual user environment where music and photographs are important and the business environment used for apps, business email, and documents. Enterprises may choose to allow employees to use their own devices for business purposes, or there may be a requirement

that IT procure and configure devices that will be used for business purposes. In either case, management of these devices is important to protect IT and corporate resources.

Configuration Manager 2012 has also changed in a significant way with the addition of support for non-Windows devices. There are two support models for devices in Configuration Manager 2012—lite management and depth management:

Lite Management Lite management is the mechanism used to manage Microsoft's own Windows Phone 7/7.5 platform and is also the management mode that supports any other device capable of working with an Exchange ActiveSync connection. This includes BlackBerry, iPhone, and Android. Lite management requires Exchange Server 2010 or Exchange Server 2013 either on-premises or in the cloud.

There is no client software installed on the device in a lite-management scenario. The management capabilities available are dependent on the capabilities of the device and what is offered via the Exchange ActiveSync connector available in Configuration Manager 2012.

Depth Management Depth management is available for traditional Windows phone platforms, Windows CE, Windows Mobile, and Nokia phones running Symbian. Depth management does install client software on the device and affords more capabilities than lite management alone; for older versions, as mentioned earlier, a client can be downloaded. For newer devices with operating systems such as Windows Mobile 8, iPhone, iPad, and Android, depth management is available through the Windows Intune connector.

We'll discuss both in detail later in the chapter. For now, it's sufficient to know that lite management will allow any device capable of communicating with Exchange Server 2010 or Windows Server 2013 through ActiveSync to be managed.

Mobile Device Management is Evolving Quickly

It's also worth mentioning that Configuration Manager 2012 R2 together with the Windows Intune service is the mobile device management solution going forward. Microsoft provides choice and flexibility in how you are able to manage your devices, either completely on-premises via Configuration Manager, cloud-based via Windows Intune, or via a hybrid model, using the Windows Intune Connector in Configuration Manager 2012 R2.

In this book we look at the on-premises and hybrid solutions. One way of adding new capabilities to the hybrid solution is done via the Extensions for Windows Intune, which you can find in the Configuration Manager 2012 R2 console.

Via the Extensions for Windows Intune node, in Administration Workspace ➢ Overview ➢ Cloud Services in the Configuration Manager console, features or supported platforms can be added without, for instance, needing to release a Service Pack for Configuration Manager 2012 R2. This is a quick and easy way to add new capabilities to your mobile device management solution.

Mobile Device Management Options

The requirements for mobile device management differ depending on whether devices are being managed using lite-management or depth-management options. For depth management you have two options: depth management with a client or depth management via the Windows Intune connector.

Let's first look at the supported operating systems and the options you have in managing them:

Android Management options:

- Windows Intune connector
- Exchange connector

Features**:**

- Settings management
- Software distribution (Windows Intune only)
- Hardware inventory
- Remote wipe/retire

Apple iOS Management options:

- Windows Intune connector
- Exchange connector

Features:

- Settings management
- Software distribution (Windows Intune only)
- Hardware inventory
- Remote wipe/retire

Nokia Symbian Belle Management options:

- Direct via client
- Exchange connector

Features:

- Settings management
- Software distribution (client only)
- Hardware inventory
- Remote wipe/retire

Windows 8.x RT Management options:

- Windows Intune connector

Features:

- Settings management
- Software distribution
- Hardware inventory
- Remote wipe/retire

Windows CE 5.0, 6.0, and 7.0 Management options:

- Direct via client
- Exchange connector

Features:

- Settings management
- Software distribution (client only)
- Hardware inventory
- Remote wipe/retire

Windows Mobile 6.0, 6.1, and 6.5 Management options:

- Direct via client
- Exchange connector

Features:

- Settings management
- Hardware inventory
- Remote wipe/retire

Windows Phone 7.x Management options:

- Direct via client
- Exchange connector

Features:

- Settings management
- Hardware inventory
- Remote wipe/retire

Windows Phone 8 Management options:

- Windows Intune connector
- Exchange connector

Features:

- Settings management
- Software distribution (Windows Intune only)
- Hardware inventory
- Remote wipe/retire

Lite Management

There are a few components required for lite management of mobile devices:

- A device capable of establishing an ActiveSync connection with an Exchange server
- An Exchange Server 2010/2013 server providing ActiveSync services, either on-premises or in the cloud
- A properly configured ActiveSync connector in Configuration Manager 2012

Configuring Required Components

The first requirement is totally dependent on the capability of the device being used—a device is either able to communicate via an ActiveSync connection or it isn't. Fortunately, most modern devices have this capability. The process of configuring the ActiveSync connection on a device may vary depending on the type of device in use. Thus, the specifics of configuring the ActiveSync connection from a device perspective are beyond the scope of discussion for this chapter.

Configuring an Exchange server to deliver ActiveSync services, the second requirement, is specifically an Exchange Server 2010 activity. There are no specific Configuration Manager requirements to consider when setting up Exchange 2010 ActiveSync. Once ActiveSync is configured and working in an Exchange Server 2010 environment, Configuration Manager can be configured to use it. How to enable ActiveSync for Exchange Server is beyond the scope of discussion for this chapter. Details on how to configure the Exchange ActiveSync component can be found with a quick Bing search. The following URLs are a good starting point to understand the setup requirements and process:

```
http://technet.microsoft.com/en-us/library/aa998357.aspx
http://technet.microsoft.com/en-us/library/bb124234.aspx
```

This leaves the third option for discussion—configuring the ActiveSync connector in Configuration Manager 2012. The ActiveSync connector option is configured from the Administration node of the console, as shown in Figure 16.1. In the console the connector is labeled Exchange Server Connectors. Note that the options available in the wizard are the only ones configurable for lite device management in Configuration Manager 2012. There may be other options for ActiveSync management available directly in Exchange Server beyond those listed in the wizard.

As shown, it's possible to have multiple connectors configured per site depending on need.

You configure a connector by right-clicking Exchange Server Connectors and selecting Add Exchange Server. This will launch the General page of the Add Exchange Server Wizard, as shown in Figure 16.2.

The first choice to make is whether the Exchange server being configured is an on-premises Exchange server or a hosted Exchange server. The connector works fine with both. In either case you must specify an FQDN for the Exchange server. When you specify On-Premises Exchange Server, you can also specify advanced configuration options. Selecting the Specify Exchange Client Access Server check box allows you to specify a specific Client Access Server (CAS) that should be used by the connector when more than a single CAS is available. If the advanced option is not specified, then Configuration Manager will simply choose a CAS to use based on information published in Active Directory.

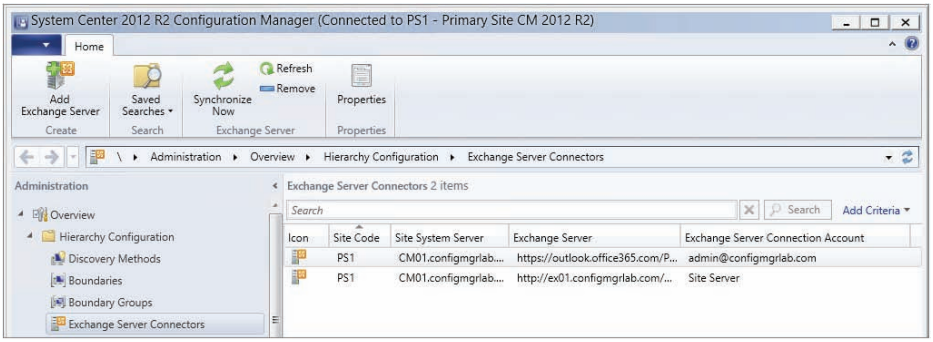


FIGURE 16.1 Exchange Server Connectors location in the Configuration Manager console

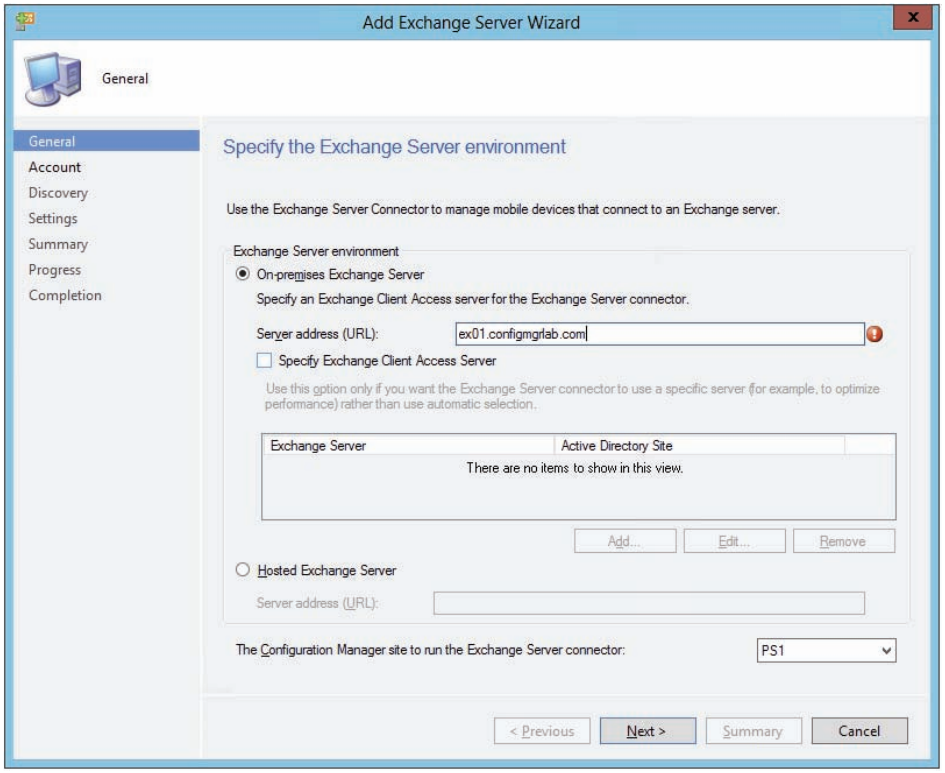


FIGURE 16.2 Add Exchange Server Wizard—General page

The last option on the General page allows you to select which Configuration Manager site the connector should be associated with. Once the configurations on this page are complete, click Next to continue to the Account page, shown in Figure 16.3.

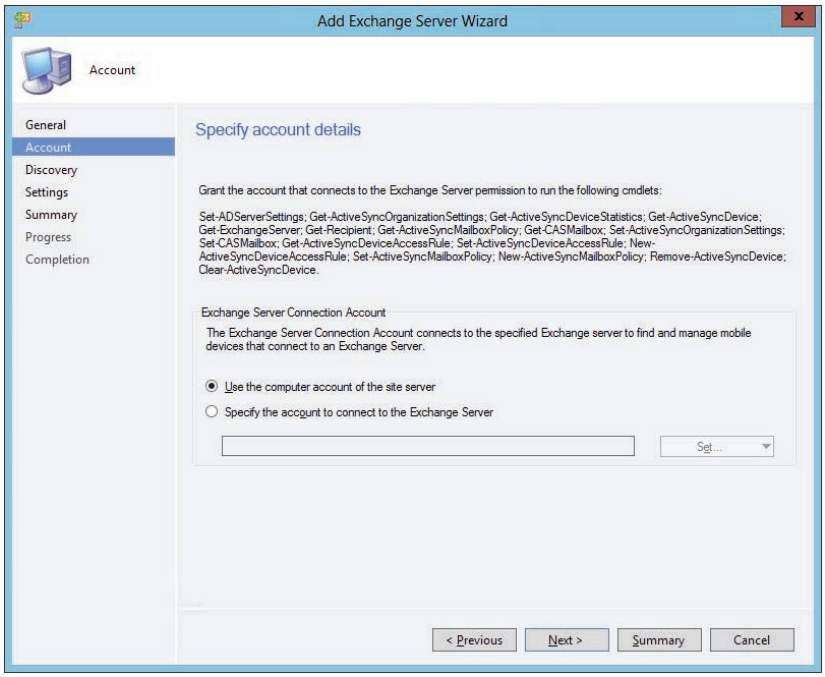


Figure 16.3
Add Exchange Server Wizard—Account page

The Account page allows administers to configure whether the Exchange Server Connection Account should be configured to use the computer account of the site server or a specific account. Regardless of the configuration you choose here, ensure that the configured account has proper rights to access the Exchange Client Access Server(s) chosen. Once configurations on this page are complete, click Next to continue to the Discovery page, shown in Figure 16.4.

The Discovery page allows administrators to determine how device discovery takes place in the environment.

Full Synchronization Schedule This option configures the schedule and frequency for full synchronization in the environment. Full synchronization gathers all properties for new and existing mobile devices. The default option is for full synchronization to run daily at midnight.

Delta Synchronization Interval (Minutes) This option configures the schedule and frequency for delta synchronization in the environment. Delta synchronization identifies new mobile devices and gathers limited changes for known mobile devices. The default option is for delta synchronization to run every 240 minutes.

Full vs. Delta

Full versus delta synchronization is similar in concept to full versus delta discovery or full versus delta collection updates.

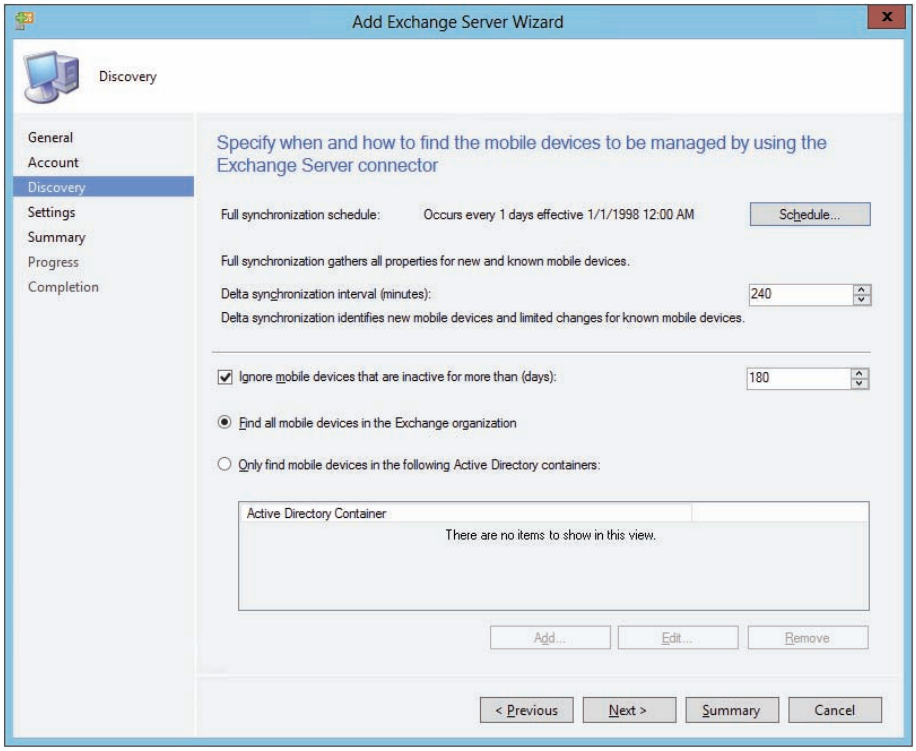


FIGURE 16.4 Add Exchange Server Wizard—Discovery page

Ignore Mobile Devices That Are Inactive For More Than (Days) This option indicates that devices that have been inactive for the configured number of days, by default 180 days, should be ignored from further management attempts.

Find All Mobile Devices In The Exchange Organization/Only Find Mobile Devices In The Following Active Directory Containers The choice you make for the first setting determines whether to attempt management of all mobile devices connecting with Exchange ActiveSync or only those belonging to a specific container. If you select to limit management, individual containers with mobile devices that should be managed must be configured.

Note that if settings are not specifically configured on this page, existing settings configured in Exchange ActiveSync will be persisted as noted by the Status column on the Settings page. If settings are configured through the connector, the Status column will change to indicate Configured By Configuration Manager. Once configurations on this page are complete, click Next to continue to the Settings page, shown in Figure 16.5.

The Settings page is where the action is! This page is the launch point for configuring all options that are available for lite management. The categories for configurable settings are General, Password, Email Management, Security, and Applications. Further discussion on these categories follows. From this page, administrators are also able to choose whether to allow external mobile device management.

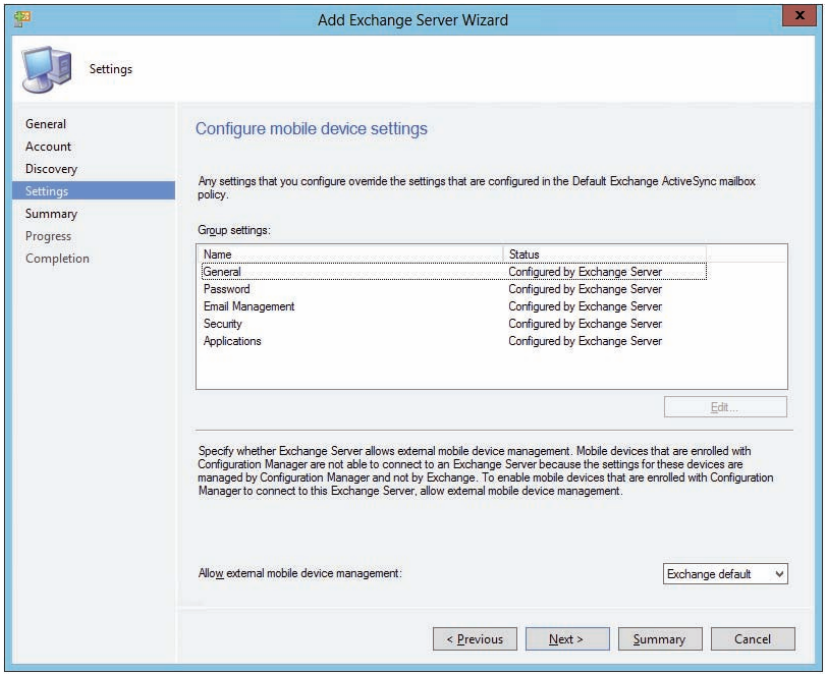


FIGURE 16.5
Add Exchange Server Wizard—Settings page

General Settings

Selecting to edit the General settings will reveal available choices for this category, as shown in Figure 16.6.

Internet Sharing From Mobile Devices This option allows administers to either allow or prohibit Internet sharing on managed mobile devices.

Computer Synchronization This option allows administers to either allow or prohibit synchronization of the mobile device with computers.

Allow Mobile Devices That Cannot Be Provisioned This option allows administrators to either allow or prohibit mobile devices that cannot be provisioned from being visible in Configuration Manager.

Refresh Interval (Hours) This option allows administrators to specify a specific refresh interval, if desired.

Password Settings

Selecting to edit the Password settings will reveal available choices for this category, as shown in Figure 16.7.

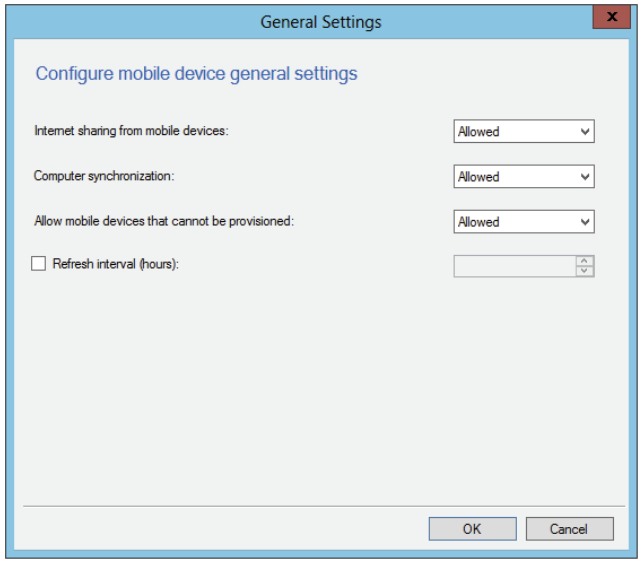


FIGURE 16.6
Add Exchange Server Wizard—Settings page—General Settings

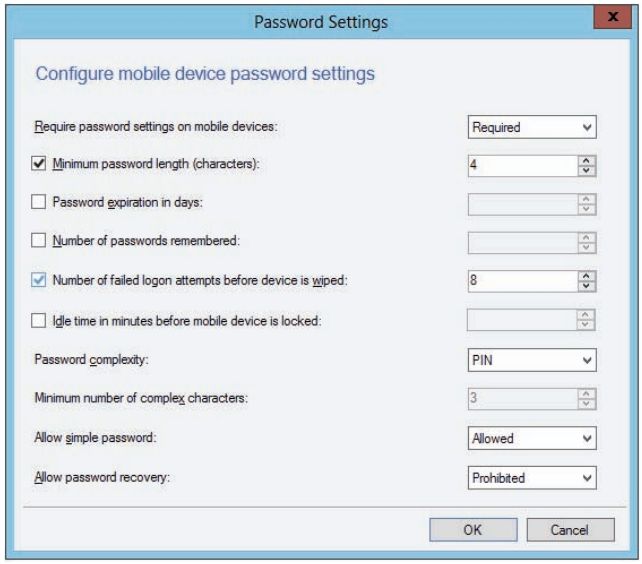


FIGURE 16.7
Add Exchange Server Wizard—Settings page—Password Settings

Require Password Settings On Mobile Devices This option allows administrators to decide whether or not to enforce password settings on the mobile device. If it's set to Optional, additional settings on this page will not be configurable.

Minimum Password Length (Characters) This option allows administrators to specify a minimum password length for the mobile device. The default length is 4 characters with a maximum length of 16 characters.

Password Expiration In Days This option allows administrators to configure how frequently the configured password will expire and need to be reset.

Number of Passwords Remembered This option allows administrators to configure how many passwords are stored, thus preventing reuse of the same password again and again.

Number Of Failed Logon Attempts Before Device Is Wiped This option allows administrators to specify the number of bad logon attempts before the device is wiped. The default is eight invalid password attempts allowed. After the configured number of failed password attempts, the device is wiped. This is a good option to use for ensuring device security, but with the result being a complete device wipe, you must carefully evaluate the final settings you choose for this option.

Idle Time In Minutes Before Mobile Device Is Locked This option allows administrators to specify the length of idle time allowed before the device will lock itself, requiring a password to regain access.

Password Complexity This option allows administrators to specify how complex the device password should be. The default option is to specify a PIN. The other option is to specify a strong password. If a strong password is selected, the option to specify a minimum number of complex characters becomes available. The default number of strong characters is three.

Allow Simple Password This option specifies whether simple passwords, such as 1234, are allowed on a device. The default option allows a simple password.

Allow Password Recovery This option allows administrators to configure whether it is possible to recover passwords on a device. The default option prohibits this action.

Email Management Settings

Selecting to edit the Email Management settings reveals available choices for this category, as shown in Figure 16.8.

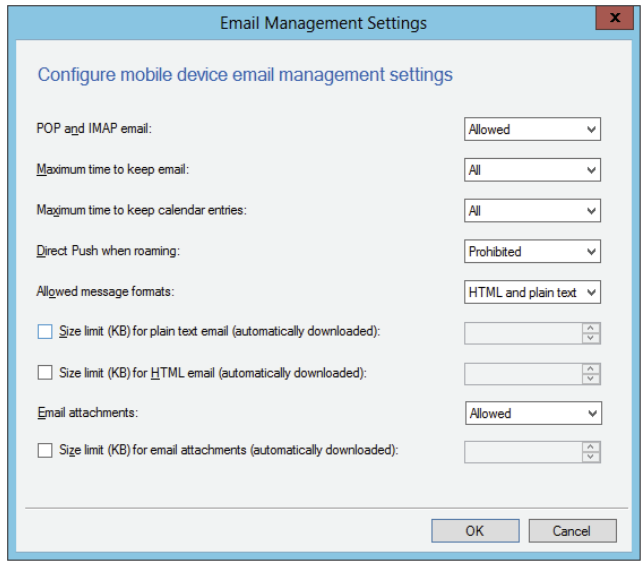


Figure 16.8
Add Exchange Server Wizard—Settings page—Email Management Settings

POP And IMAP Email This option allows administrators to specify whether both POP and IMAP email are allowed or prohibited. There is no option to specify that one or the other is available.

Maximum Time To Keep Email This option allows administrators to specify the length of time email will be retained on the device. The default option is All, which indicates that all email should be retained indefinitely. Other available options are One Day, Three Days, One Week, Two Weeks, and One Month.

Maximum Time To Keep Calendar Entries This option allows administrators to specify the length of time calendar entries should be retained on the device. The default option is All, which indicates that all calendar items should be retained indefinitely. Other available options are Two Weeks, One Month, Three Months, and Six Months.

Direct Push When Roaming This option allows administrators to determine whether email can be directly pushed while a device is in roaming status. The default option is Prohibited to help avoid additional expense in such situations.

Allowed Message Formats This option allows administrators to define what email formats are acceptable. The default option is HTML And Plain Text. The only other choice is Plain Text Only.

Size Limit (KB) For Plain Text Email (Automatically Downloaded) If specified, this option allows administrators to specify the maximum size for a plain text email that will be automatically downloaded to devices.

Size Limit (KB) For HTML Email (Automatically Downloaded) This option, not specified by default, allows administrators to specify the maximum size for an HTML-formatted email that will be automatically downloaded to devices.

Email Attachments This option allows administrators to specify whether email attachments are allowed on connected devices. The default option is Allowed.

Size Limit (KB) For Email Attachments (Automatically Downloaded) This option, not specified by default, allows administrators to specify the maximum size for an attachment that will be automatically downloaded to devices.

Security Settings

Selecting to edit the Security settings will reveal available choices for this category, shown in Figure 16.9.

Remote Desktop This option allows administrators to specify whether Remote Desktop to the device is allowed.

Removable Storage This option allows administrators to specify whether removable storage is allowed on the device.

Camera This option allows administrators to specify whether the use of the camera is allowed on the device.

Bluetooth This option allows administrators to specify whether the use of Bluetooth is allowed on the device. An option is included in this setting to allow configuring hands-free operation only for Bluetooth.

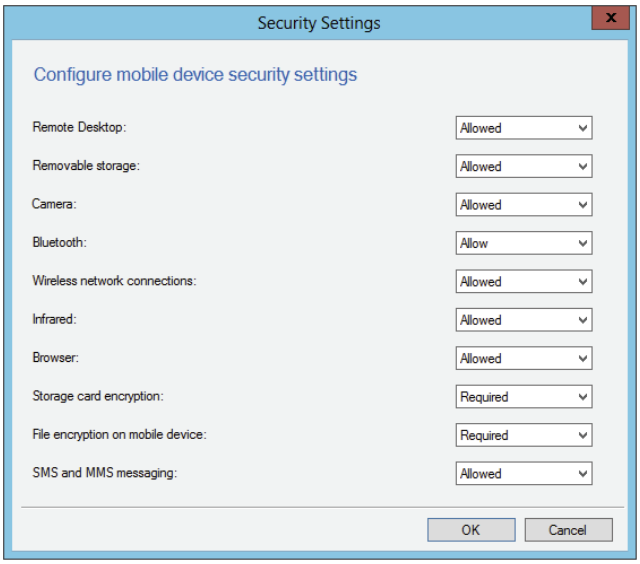


FIGURE 16.9
Add Exchange Server Wizard—Settings page—Security Settings

Wireless Network Connections This option allows administrators to specify whether the use of wireless network connections is allowed on the device.

Infrared This option allows administrators to specify whether the use of infrared capabilities for a device is allowed.

Browser This option allows administrators to specify whether the use of a browser is permitted for a device.

Storage Card Encryption This option allows administrators to configure whether encryption of device storage cards is required or optional.

File Encryption On Mobile Devices This option allows administrators to configure whether file encryption on mobile devices is required or optional.

SMS And MMS Messaging This option allows administrators to configure whether messaging is allowed on devices.

Applications Settings

Selecting to edit the Applications settings will reveal available choices for this category, shown in Figure 16.10.

Unsigned File Installation This option allows administrators to specify whether installation of unsigned files is allowed on devices.

Unsigned Applications This option allows administrators to specify whether installation of unsigned applications is allowed on devices.

Block The Following Applications In ROM This option allows administrators to specify a list of applications that should be blocked from being installed on the device.

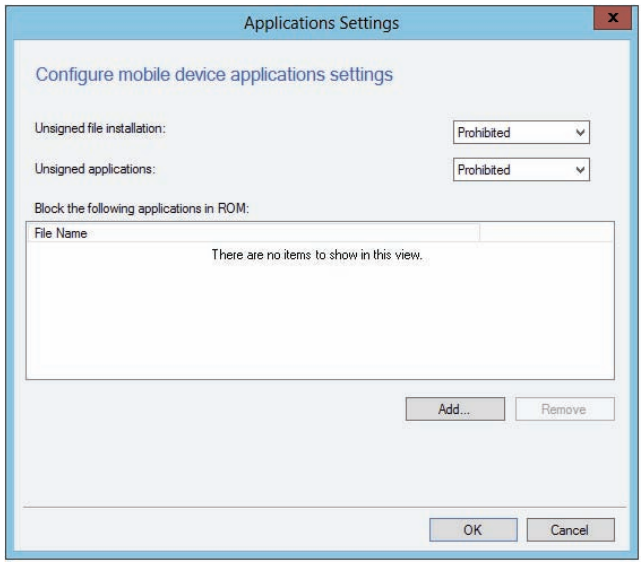


FIGURE 16.10
Add Exchange Server Wizard—Settings page—Application Settings

RESULTS OF LITE-MANAGEMENT CONFIGURATION

Once all settings are configured as required on these pages, click Next and continue through the wizard, verifying on the Summary page that all options chosen are appropriate. This action implements the settings as required on the Exchange server, and from this point devices connecting to Exchange Server through ActiveSync will receive and implement the configured settings, or at least the ones the device is capable of implementing.

After a few devices have synchronized using the ActiveSync connector, they will be visible and available for management in the Devices collections, as shown in Figure 16.11.

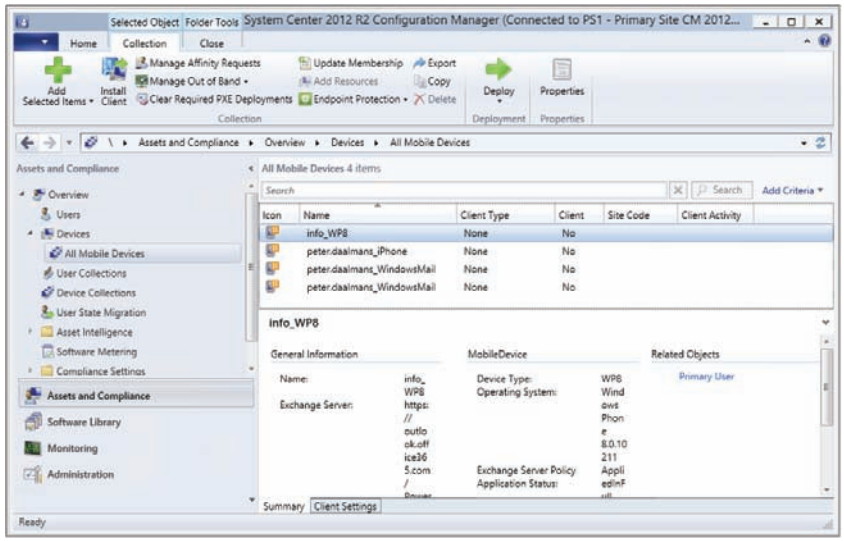
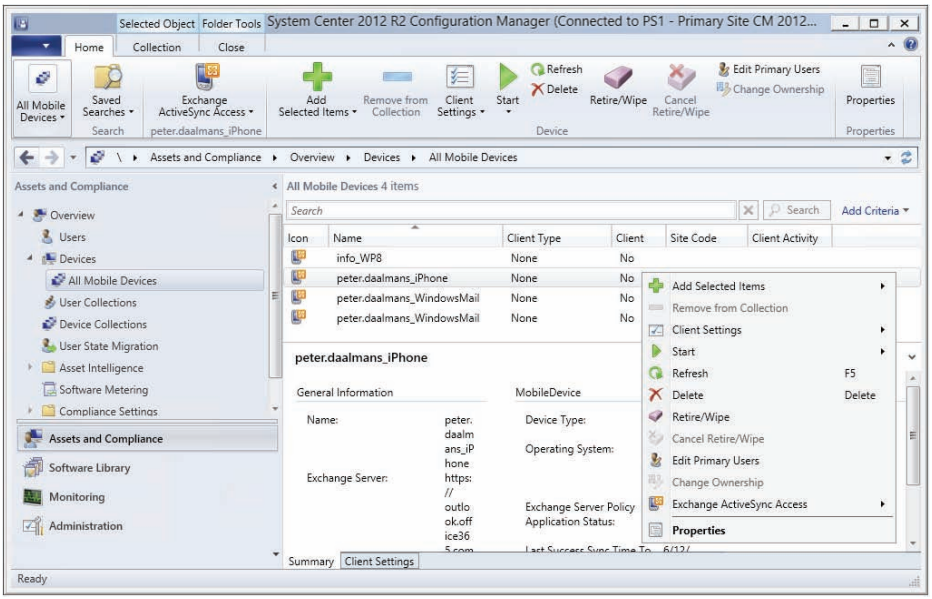


FIGURE 16.11
Lite-managed devices

Now that devices are in collections, is it possible to do any management directly at this level? Mostly *no*. Remember, these devices are lite managed, which means almost all management is done through the ActiveSync connector. There are a couple of things that you can do, though. Right-clicking a lite-managed device will show the options available. Specifically there are options to wipe the device and also to decide whether to block the device. This is also the location to set the primary device user, to open Resource Explorer for the device to view hardware inventory that has been collected, and also to view device properties. These options are shown in Figure 16.12.

FIGURE 16.12
Device context menu options



Depth Management via Client

In Configuration Manager 2012 R2 you have two ways of providing depth management: depth management via installing a client directly on a (legacy) mobile device like Windows Phone 7 and Nokia Symbian devices or depth management via the Windows Intune connector.

Let's first look at the old-fashioned way. In this scenario, some components are required and others are optional but likely needed:

Required roles

- Enrollment proxy point site system role
- Enrollment service point site system role
- Management point configured for HTTPS communication
- Microsoft enterprise certification authority

Optional roles—depending on services being provided

- Distribution point configured for HTTPS communication
- Application Catalog web service point

We describe configuring both the required and optional roles in detail in the following sections and end with discussions of depth-management device enrollment and device-settings management.

Enrollment Proxy Point Site System Role

This site system role is used by devices during initial enrollment and client installation. This is also the site system role contacted to initially download the client for depth-managed devices.

This role is configured in the DMZ and must be configured with a web server certificate from the certification authority. Installing the enrollment proxy point site system role is straightforward; simply select the server that will host the role in the Administration ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles node of the console, choose to add a new site system role, and select Enrollment Proxy Point from the list. The only configurations needed for this role are shown in Figure 16.13.

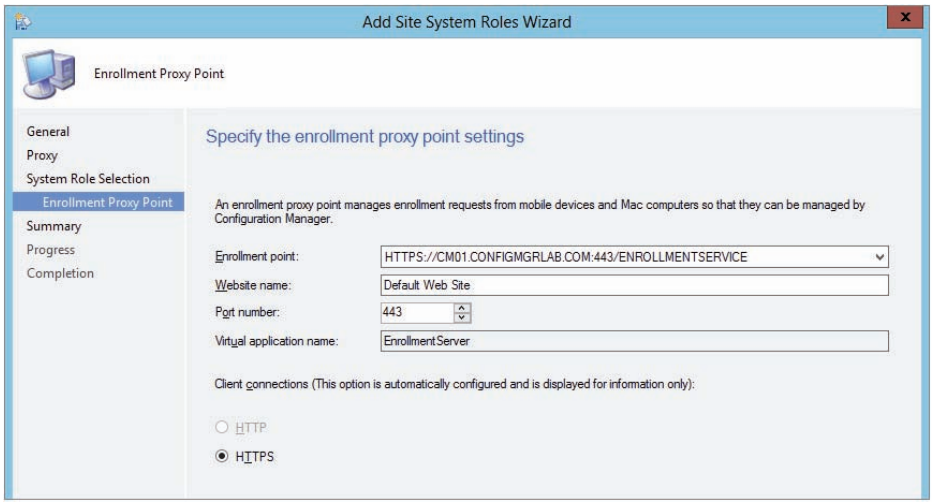


Figure 16.13 Enrollment proxy point site system role settings

Enrollment Point This setting allows administrators to configure the URL for the enrollment point. Typically this should be left at the default value.

Website Name This setting allows administrators to configure the website where the enrollment proxy point should be installed. The default is to use the default website. Often, organizations will require a website other than the default website, particularly in the DMZ. If this is the case, specify which website should host the enrollment proxy point.

Port Number This setting allows administrators to specify the port that should be used to connect with the enrollment proxy point. Using port 443 is typical, but this is user configurable if needed.

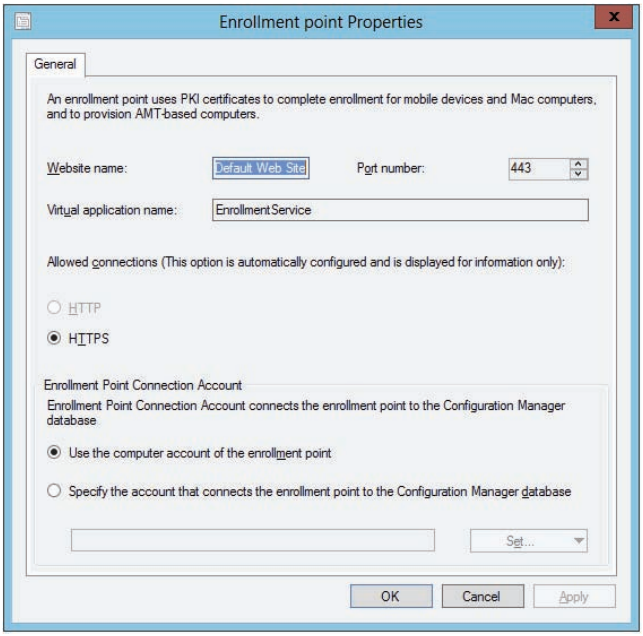
The remaining options on this page, Virtual Application Name and Client Connections, are displayed but are not user configurable.

Enrollment Point Site System Role

This site system role resides on the internal network, receives information from the enrollment proxy point, and interacts with the primary site server, Active Directory, and the certification authority to orchestrate the device-provisioning process. The server hosting this role must be provisioned with a web server certificate from the internal certification authority.

Installing the enrollment point site system role is straightforward; simply select the server that will host the role in the Administration ➢ Overview ➢ Site Configuration ➢ Servers And Site System Roles node of the console, choose to add a new site system role, and select Enrollment Point from the list. The only configurations needed for this role are shown in Figure 16.14.

Figure 16.14
Enrollment point site system role settings



Website Name/Port Number This option allows administrators to configure the website name to be used for installing the enrollment point. The default is to use the default website. Some organizations disable the default website as a matter of policy. If this is the case in your

organization, choose an appropriate alternative. The port number is also listed as an option and defaults to port 443. This setting will be unchanged in most environments but is user configurable if needed.

Virtual Application Name This option allows administrators to specify the virtual application name if different from the default.

The Enrollment Point Connection Account This option allows administrators to specify which account should be used to facilitate communication from the enrollment point to the primary site server. If the enrollment point is collocated on the primary site server, it is typical to allow the computer account to be used for communication. If the site system is remote, it's possible to use the computer account of the remote site system, provided appropriate rights are granted on the primary site server. In the remote scenario it's often easier to specify an account to use. One key deciding factor might be account password maintenance requirements. In the case of the computer account, the password is managed automatically. For user accounts, password management is manual.

The remaining option on this page, Allowed Connections, is displayed but is not user configurable.

Management Point

A management point is required for any primary site that will host clients. Managing devices also requires a management point configured to allow mobile devices to connect as well. Figure 16.15 shows the Properties page for the management point. You'll need to adjust a couple of items if the management point will support device clients.

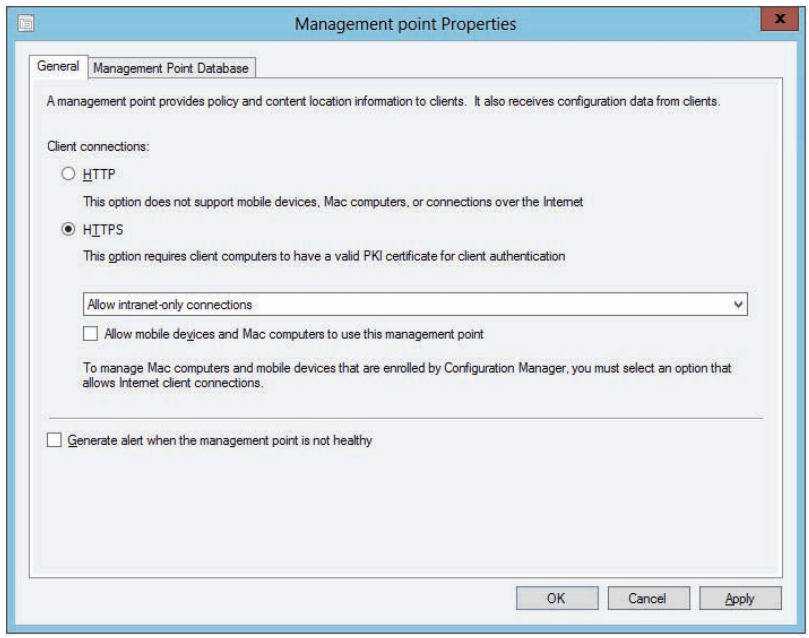


Figure 16.15
Management Point Properties page

Management points purposed for device management must be configured for HTTPS communication and, accordingly, must have a web server certificate from the configured certification authority installed. Further, the check box Allow Mobile Devices And Mac Computers To Use This Management Point must be selected.

When you decide on the placement and configuration of management points, you should consider the available configuration options as for client connections:

HTTP Devices connected via HTTP are typically located on the internal network. A management point purposed to support this type of device cannot also be configured to support mobile devices unless all connected computers are reconfigured to use HTTPS communication and the management point configuration is updated accordingly.

HTTPS Any management point can be configured to communicate with clients using HTTPS, whether the computer devices are on the internal or external network. In fact, using HTTPS communication is the most secure way to configure client/management point interaction. If a management point is configured in this way and mobile devices are also available that need to be managed, simply check the box to allow the management point to also serve mobile devices.

Microsoft Enterprise Certification Authority

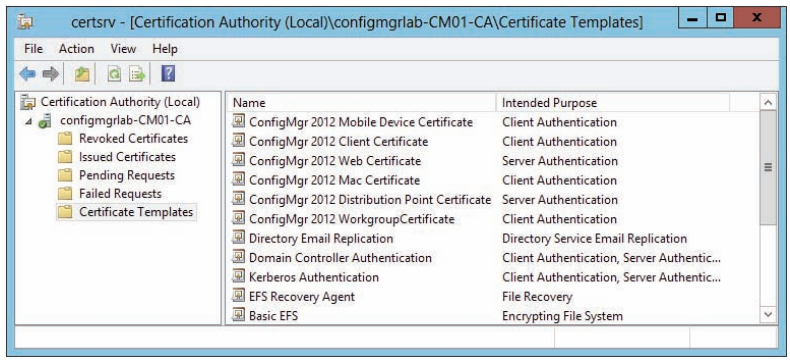
Mobile devices require certificates to communicate and be approved in the environment. Certificates are a topic that seems to bring hesitation and uncertainty for many Configuration Manager administrators—often either because the topic of certificates isn't familiar or the use of certificates might involve dependency on another operational team in the organization. Oftentimes it seems easier to just do it yourself than involve other teams! Don't let either of these prevent you from using certificates—it's really not difficult to do, and the added security and flexibility it brings is worth the time.

Discussing configuration of a certification authority is beyond the scope of this chapter—not to mention the fact that any discussion may or may not line up with specific organizational requirements. Documentation that walks through the process of deploying required certificates in a lab environment to afford testing of mobile device management is available at the following link:

```
http://technet.microsoft.com/en-us/library/gg682023.aspx
```

Figure 16.16 shows a screenshot of a certification authority configured to deploy the needed certificates for mobile device management.

Figure 16.16
Certification authority



Distribution Point

Distribution points purposed for device management must be configured for HTTPS communication and, accordingly, must have a web server certificate from the configured certification authority installed. Making distribution points available for access by mobile devices means placing the distribution point in the DMZ. Because of this requirement and the different content required by devices, distribution points for access by mobile devices may be kept separate from those accessed by computer devices. Figure 16.17 shows distribution point properties used to enable HTTPS communication.

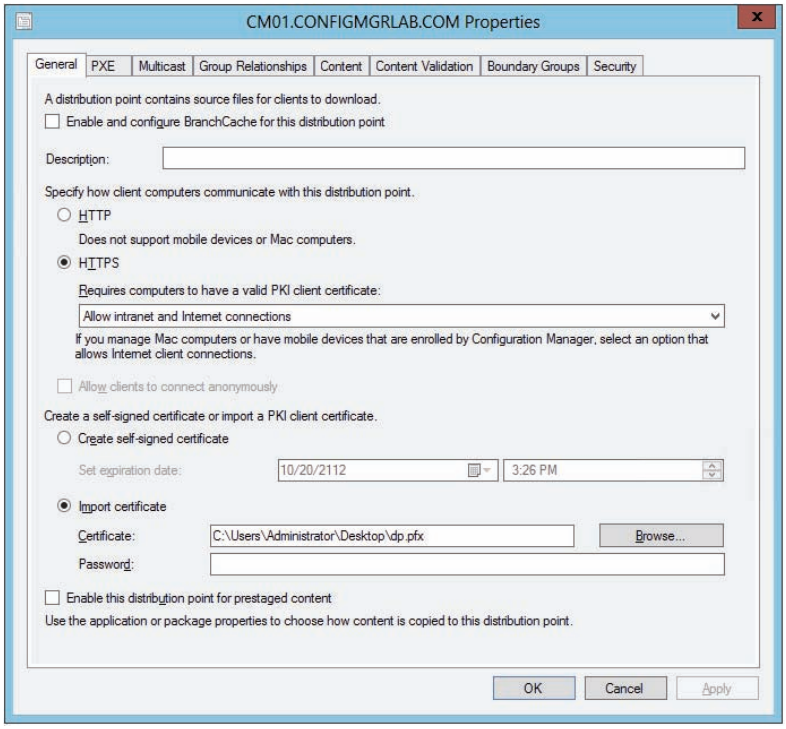


Figure 16.17
Distribution point Properties page

Application Catalog Web Service Point

The Application Catalog web service point is an optional site system role for use by mobile devices but is required to provide the mobile device user with the ability to wipe their own device. Like other roles, configuring the Application Catalog point for use by mobile devices requires the use of HTTPS communication, which requires that a web server certificate from the local certification authority be configured. Figure 16.18 shows the HTTPS configuration option for the Application Catalog web service point.

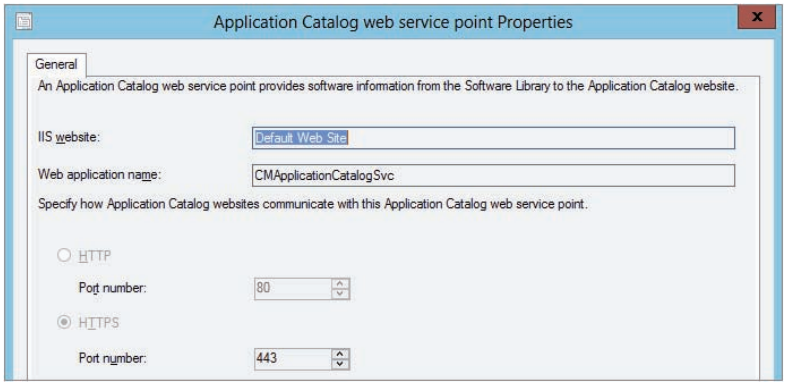


Figure 16.18
Application Catalog Web Service Point Properties page

Depth-Management Device Enrollment

The enrollment process and provisioning process require action from both the device user and the Configuration Manager administrator. The administrator portion of the configuration must be in place prior to user involvement, so our discussion will focus there first.

Administrator Configuration

The administrator must decide which users can participate in device enrollment and provisioning. This is done by configuring the client settings. The option to enable mobile device enrollment is a user setting that is available either by configuring the Default Client Settings, which combine both default user and device settings for the site, or by choosing to configure a custom settings profile for users. The Default Client Settings should be used when device enrollment should be enabled for all users, while the custom settings profile should be used where enrollment rights should be granted only to select users. The example will demonstrate the latter option:

1. To configure user-specific enrollment options, create custom user settings and enable enrollment, as shown in Figure 16.19.

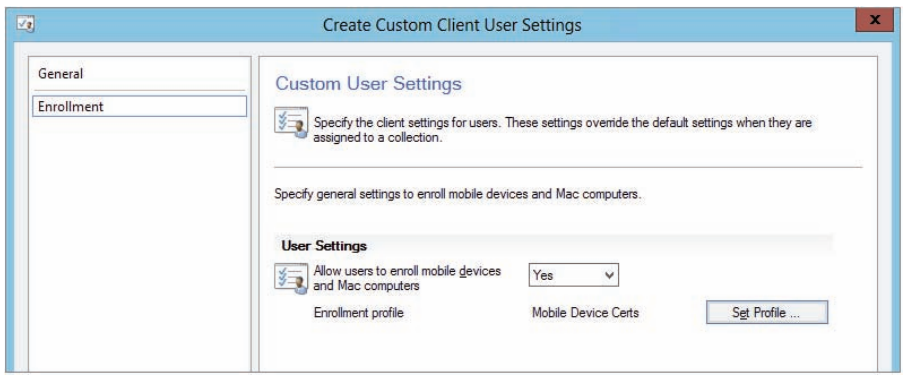


Figure 16.19
Custom user settings to enable enrollment

2. Configure a user collection that contains all users who should be granted the right of device enrollment.

   This collection can consist of either individual users or groups of users.

3. With both of these items created, it's a matter of linking the two. Simply go back to the custom user settings and assign them to the collection just created, as shown in Figure 16.20.

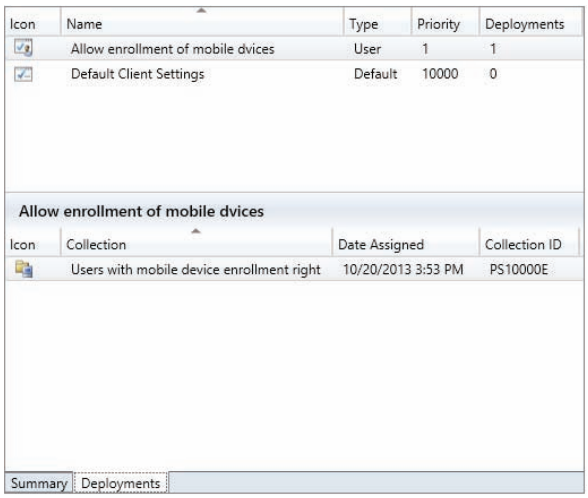


FIGURE 16.20
Custom user settings assigned to device enrollment collection

   Complete the assignment process by right-clicking the custom setting and selecting Assign. It is also possible to link custom settings to more than a single collection.

This configuration of appropriate site systems and appropriate client settings is all that is required in order to enroll and provision devices. There is more work for the administrator to do in terms of configuring settings that should be in place on the various devices, but we'll cover that later.

User Configuration

Actions required from the device user's perspective are straightforward. The actual enrollment process behind the scenes is a bit more involved. The device user will need to do only two things: Install some software and enter credentials.

You can obtain the Enterprise Enrollment software from the enrollment web proxy site system by directing the device's web browser to the URL for this site system. The default URL is

```
https://<enrollmentwebproxyservername>/EnrollmentServer
```

It's also possible that the Enterprise Enrollment software could be made available through another means, such as an email link. Regardless of the mechanism used to deliver the Enterprise Enrollment software to the device, it must be installed. In the example scenario, we obtain the software by browsing to the enrollment web proxy site system. Figure 16.21 shows the user being prompted for what action to take when presented with the enrollment software.



FIGURE 16.21
User prompted for action regarding enrollment software

For the example, we saved the software to the device before running it. This is shown in Figure 16.22.



FIGURE 16.22
Select a location for the enrollment software

Once you've downloaded the software, you can find it in the root folder when viewing File Explorer on the device. For the example, do the following:

1. Locate the software and select it to begin the installation process. Figure 16.23 shows the installation process.



FIGURE 16.23
Enrollment software installing to the device

Once it is installed, the enrollment software should automatically launch. If it doesn't, you can initiate it from the Start menu, as shown in Figure 16.24.



FIGURE 16.24
Enrollment software installed and available on the Start menu

2. Once it is launched, review the text and click Enroll, as shown in Figure 16.25.
3. Provide an email address, password, and server address on the credentials screen, as shown in Figure 16.26.



Figure 16.25
Beginning the enrollment process



Figure 16.26
Credentials screen of the enrollment wizard

By default the option Use The Default Enrollment Server is selected. In the example scenario, the default configuration was inaccurate. Once you've provided the details, click Next.

A Few Words about Email Lookup and User Accounts

The email address is used to look up the proper domain account. Once looked up, the actual account in `domain\user` format is used for verifying credentials. You can see this in the enrollment logs, discussed later.

From here, it's possible the user will see a warning screen regarding the site's certificate.

4. If so, verify that the certificate is OK, and click Yes to continue.

The enrollment process begins. To the device user, the process is fairly boring, as shown in Figure 16.27.

FIGURE 16.27
Enrollment in progress



In reality, there is a lot going on behind the scenes. In brief, the process is as follows:

1. The enrollment web proxy point takes the information supplied and passes it to the enrollment service point.
2. The enrollment service point forwards the information to the primary site for evaluation. This evaluation confirms that the user has been granted rights to enroll their device in the site.
3. Assuming the user is approved, the enrollment service point will contact the enterprise certification authority to retrieve the needed certificate and send that back to the device through the enrollment web proxy point.

After this process completes, the device is enrolled and ready to be provisioned and managed. This is shown in Figure 16.28.

Once the enrollment process is complete, there will be a delay before the device will be fully managed by the site—sometimes as long as eight hours. After this period the device should show up in the All Mobile Devices collection as Active, as shown in Figure 16.29.

The device should also have inventory information associated with it. This is another sign that it is properly configured and is shown in Figure 16.30.

Previous versions of Configuration Manager separated device client settings from computer client settings. Configuration Manager 2012 unifies these settings so that, where applicable, the same values apply equally to all device types. Just remember that not all of the available settings are applicable to mobile devices. As an example, mobile devices are able to participate in hardware inventory as well as software distribution, but mobile devices do not submit software inventory. It is also possible to extend the hardware inventory for devices by modifying hardware inventory classes, which you are able to change in the Hardware Inventory section of the client settings.



Figure 16.28
Installation and enrollment process complete

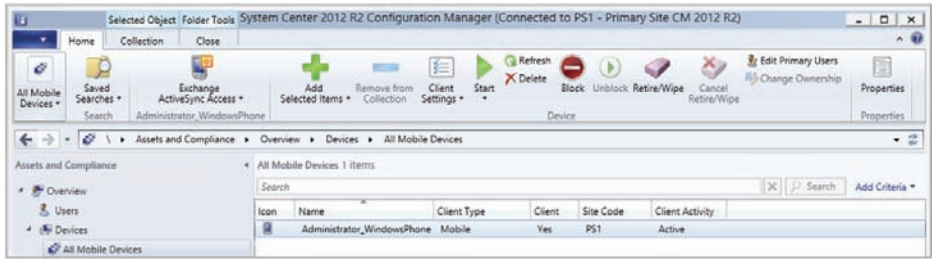


Figure 16.29
Device in Active status after enrollment and provisioning

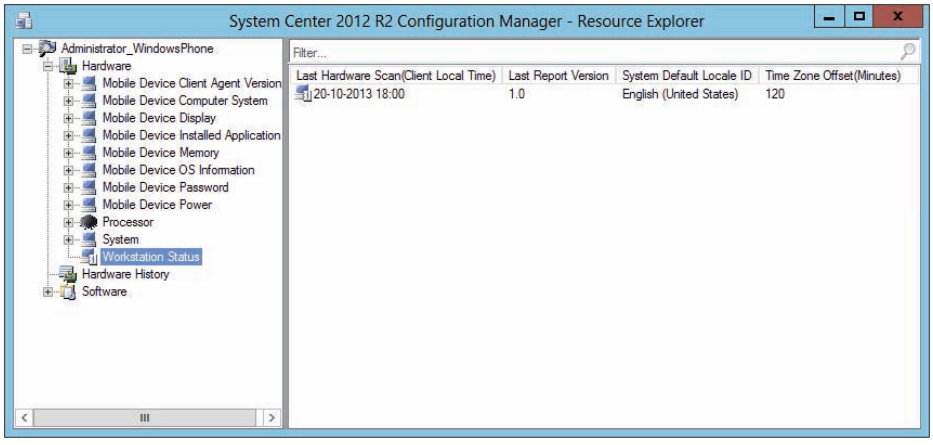


Figure 16.30
Device inventory

As mentioned, besides this way of managing legacy mobile devices, Configuration Manager 2012 R2 provides depth management via the Windows Intune connector.

Depth Management via Windows Intune

Windows Intune is a cloud service that allows you to manage your mobile devices via Configuration Manager 2012 R2. Windows Intune is used as a middle tier for you to be able to keep in touch with your mobile devices without installing a complete infrastructure in a DMZ.

Prerequisites for Windows Intune

To be able to use the depth management option via Windows Intune, you must meet some prerequisites:

- Acquire a Windows Intune subscription.
- Configure your domain name in Windows Intune.
- Add an alternative UPN suffix to your Active Directory domain (optional).
- Synchronize your users with Windows Azure Active Directory.

Acquire a Windows Intune Subscription To be allowed to use the Windows Intune cloud service, you need to acquire a Windows Intune subscription. This can be done via `www.windowsintune.com` or a Microsoft Partner. You can also register a 30-day trial subscription.

Configure Your (External) Domain Name in Windows Intune When you have access to a Windows Intune subscription, your organization account that is created while registering looks like <username>@<domainname>.onmicrosoft.com. To create a user-friendly way of logging on to the company portal, you want to add your public domain name that is used for your email. Setting up your own domain name is done by following the next steps:

1. Go to your Admin page via `https://account.manage.microsoft.com/` and log on with your Windows Intune administrator username.
2. Under Admin Overview select Domains, as shown in Figure 16.31.
3. Click Add A Domain, supply your domain name, and click Next.
4. Before Microsoft will add your domain name, you need to prove that it is really yours. You can do this by adding a TXT or MX record in your public DNS zone. Add the TXT value (for example, MS=ms201111197) to your public DNS zone and click Verify.
5. When verification is done successfully, you will see a message that the domain has been added to your account. Click Close. Your domain is now listed with a status of Verified.
6. To support enterprise enrollment, you need to set up a CNAME DNS record that redirects enterpriseenrollment.<your domainname> (for example, enterpriseenrollment.masteringsccm.com) to manage.microsoft.com.

Add an Alternative UPN Suffix to Your Active Directory Domain If you have an Active Directory domain name that is only used internally, such as any .LOCAL or .LAN domain name, and your email domain name differs from Active Directory, you may need to add an alternative Universal Principal Name (UPN) suffix to your Active Directory, as follows.

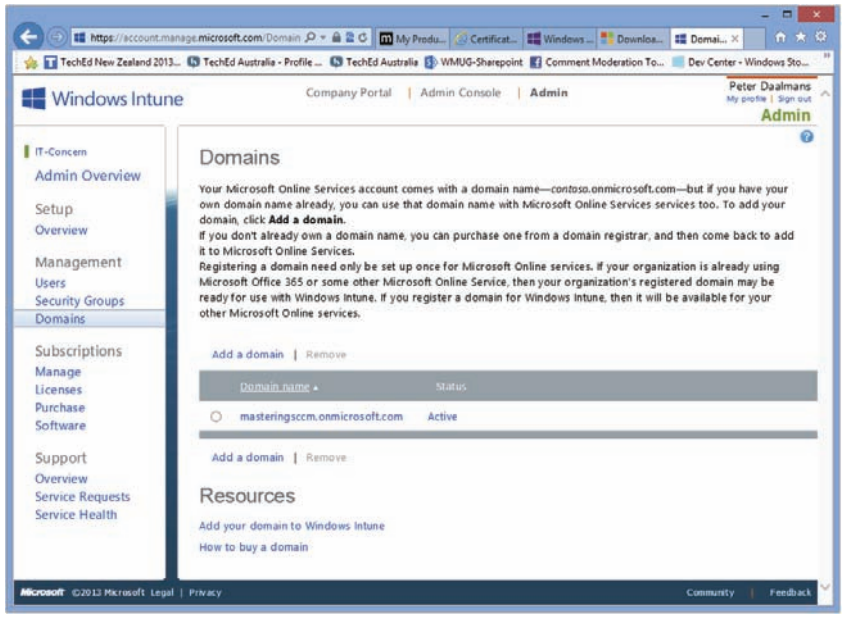


FIGURE 16.31
Domains page in Windows Intune

1. Log on to your domain controller or server with the Active Directory management tools, and from the Start menu or Start screen open the Active Directory Domains And Trusts management console.
2. Right-click Active Directory Domain And Trusts and click Properties.
3. Supply your domain name in the Alternative UPN Suffixes field and click Add, as shown in Figure 16.32.
4. Click OK.

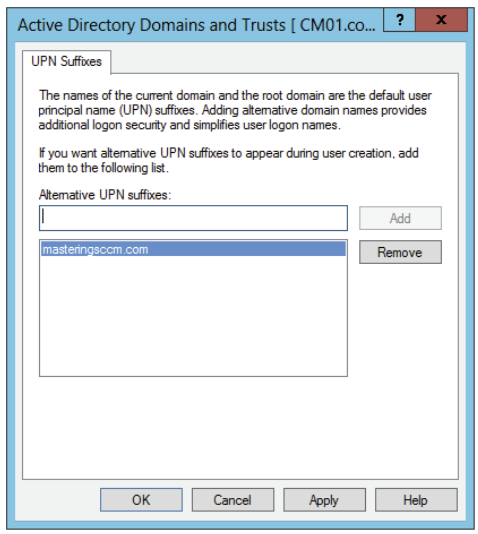


FIGURE 16.32
Add an alternative UPN suffix.

Synchronize Your Users with Windows Azure Active Directory The next step in preparing your environment for Windows Intune is setting up Active Directory synchronization. Synchronize your local Active Directory accounts to the Windows Azure Active Directory so that they can be used with Windows Intune. Follow these steps to set up Active Directory synchronization.

1. Log on to your Windows Intune admin portal (`https://account.manage.microsoft.com/`), select Users, and click Set Up next to Single Sign-on.
2. Your Internet browser will show 10 steps for setting up and checking Single Sign-on and Active Directory synchronization. You can see these steps at `https://account.manage.microsoft.com/IdentityFederation/IdentityFederation.aspx`; configure your system as described. The following global steps are described in detail.
3. Download the latest version of the Microsoft Online Services Sign-In Assistant and install the downloaded `msoidcli_64bit.msi` file with the default settings.
4. Install the Windows Azure Active Directory Module for Windows PowerShell by installing `AdministrationConfig-EN.MSI` on your server that will host single sign-on and directory synchronization services.
5. Click Activate twice on the website mentioned in step 2 of this procedure. After clicking the Activate button for Active Directory synchronization, download and install the Active Directory Sync Tool.
6. Install `dirsync.exe`, which may take 10 minutes or longer, accept the defaults, and start the Configuration Wizard by clicking Finish once the installation is finished.
7. Click Next and supply the organization account of Windows Intune, supply the password as shown in Figure 16.33, and click Next.



FIGURE 16.33 Configure the Microsoft Online Services credentials.



Real World Scenario

Disable the Password Change Requirement of the Organization Account of Windows Intune

By default a Windows Intune account password expires every 90 days. Since Configuration Manager 2012 R2 is using your organization account to connect to Windows Intune, you might need to reconfigure your Windows Intune connector every 90 days. Follow the next steps to make sure the password of the organization account does not expire. Be sure to set it with a very strong password.

1. Add the Windows Azure Active Directory Module for Windows PowerShell, and load it within Windows PowerShell.
2. Connect to Windows Azure by executing the following command:

   ```
   Connect-MsolService
   ```

3. Supply the username and password of the organizational account, and click OK to connect to Windows Azure Active Directory.
4. To enable the Password Never Expires property of the organizational account in Windows Azure Active Directory, you need to execute the following command. In this example the organizational account is `admin@masteringsccm.onmicrosoft.com`; replace this with your own account.

   ```
   Set-MsolUser -UserPrincipalName admin@masteringsccm.onmicrosoft.com
   -PasswordNeverExpires $True
   ```

5. Supply the name of a user account that has the Domain Admins and Enterprise Administrator Active Directory permissions in the User Name field, and click Next.
6. On the Hybrid Deployment page click Next, and select Enable Password Sync on the Password Synchronization page.
7. Click Next, and after the configuration completes, click Next again. Start the synchronization of the directories by enabling the Synchronize Your Directories Now option. Click Finish.

Enabling Windows Intune Connector

After the synchronization and the single sign-on are configured, you need to connect Configuration Manager 2012 R2 with the Windows Intune cloud service. Enabling the Windows Intune connector is done from the Configuration Manager 2012 R2 console. Follow these steps to enable the Windows Intune connector:

1. Open the Configuration Manager 2012 console, select the Administration workspace, and expand Overview ➢ Cloud Services ➢ Windows Intune Subscriptions.
2. Click Add Windows Intune Subscription in the Home tab of the ribbon. Click Next after reading the Introduction page of the Create Windows Intune Subscription Wizard.
3. Click Sign In, and on the Set The Mobile Device Management Authority screen, select I Understand That After I Complete The Sign-in Process, The Mobile Device Management Authority Is Permanently Set To Configuration Manager And Cannot Be Changed, as shown in Figure 16.34. Then click OK.

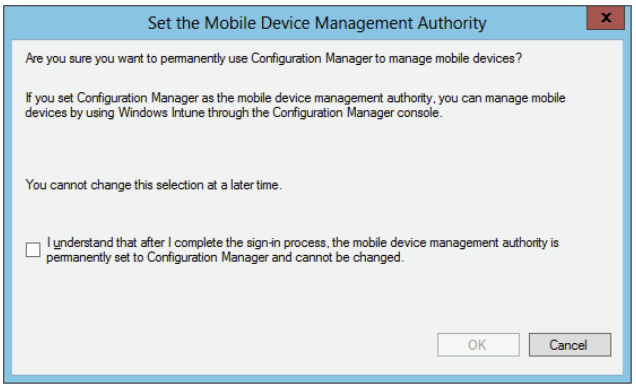


FIGURE 16.34
Set the mobile device management authority to Configuration Manager.

4. If you run this wizard from a Windows Server 2012 R2 operating system, you will probably get warnings from Internet Explorer that the content within this application is coming from the website listed and is being blocked by Internet Explorer Enhanced Security Configuration. Add the websites to the trusted sites by clicking Add twice.
5. After all websites are trusted you will reach the sign-in page of Windows Intune, as shown in Figure 16.35. Supply your organization's Windows Intune account name and the password, and click Sign In.

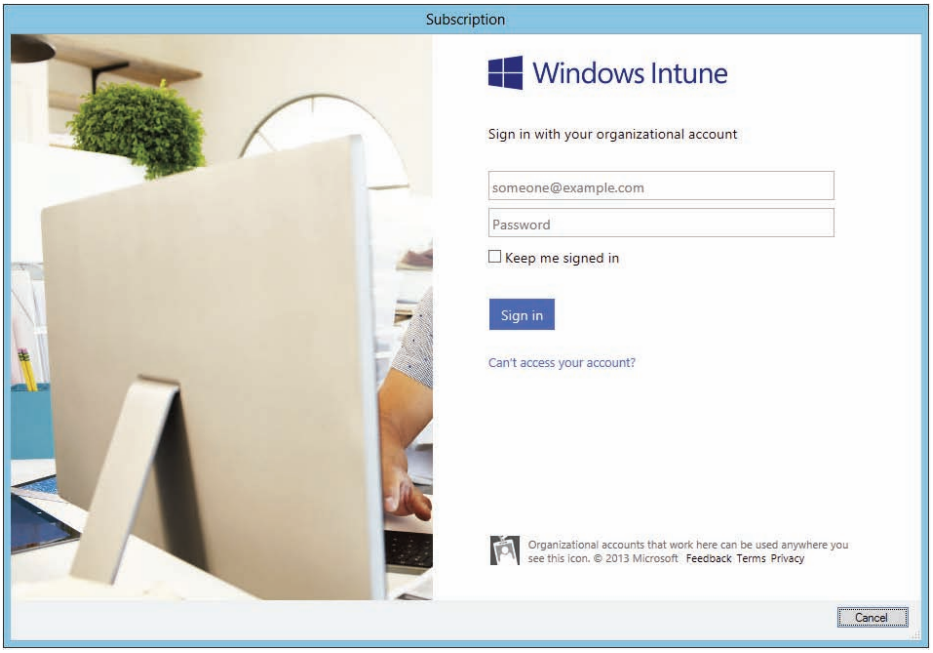


FIGURE 16.35
Windows Intune sign-in page

6. Back in the Create Windows Intune Subscription Wizard you will notice that the Sign In button is grayed out. Click Next to continue.

7. On the General Page, shown in Figure 16.36, you need to specify a user collection that allows its members to enroll their devices in Configuration Manager 2012 R2. Supply a company name, the URL to the company privacy documentation, and a color scheme for the company portal. If you have more than one Configuration Manager site in your hierarchy, specify the Configuration Manager site code.

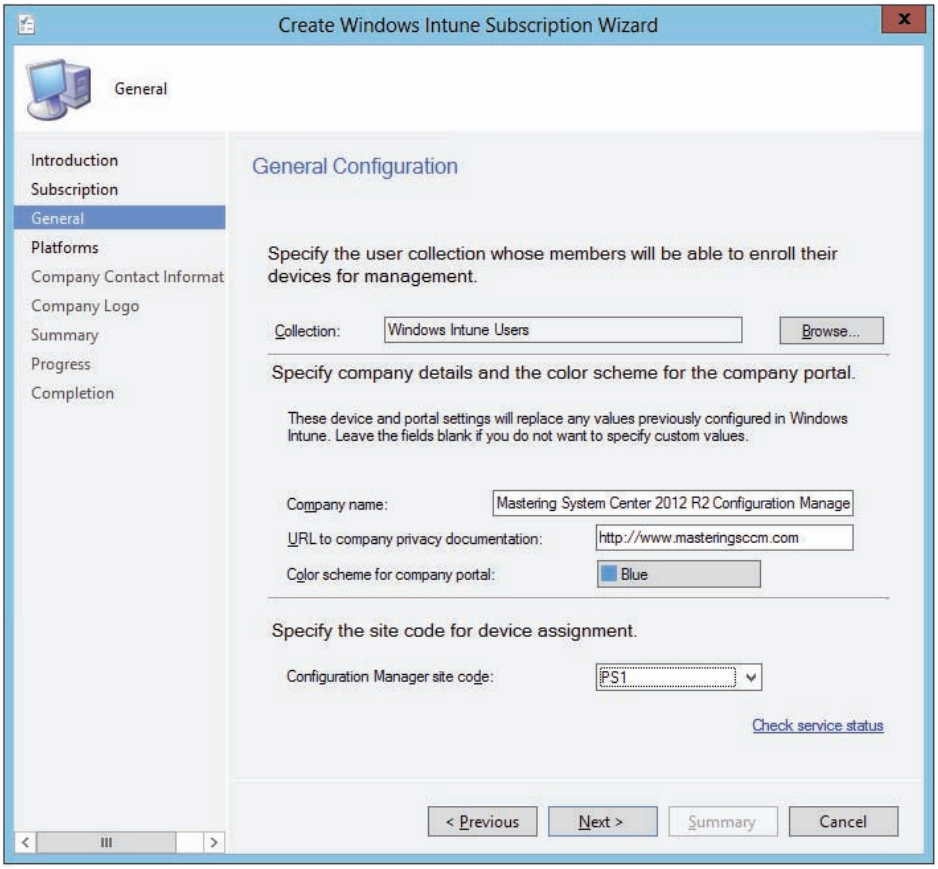


Figure 16.36
General page of the Create Windows Intune Subscription Wizard

8. The Windows Intune connector supports devices with several different operating systems, as shown in Figure 16.37.



FIGURE 16.37 Platforms page of the Create Windows Intune Subscription Wizard

Android To enable users to enroll their Android device just check Enable Android Enrollment.

iOS To support iOS enrollment you need to specify the Apple Push Notification service (APNs) certificate. This is done in three steps:

a. Create and download a Certificate Signing Request from Windows Intune. This is done in the Configuration Manager console by navigating to Administration ➢ Overview ➢ Cloud Services ➢ Windows Intune Subscriptions and clicking Create APNs Certificate Request. Supply a filename and click Download. Log into Windows Intune, and the CSR file will be saved at the configured file location. Click Close.

b. Go to the Apple Push Certificate Portal and log on with your Apple ID. Click Create A Certificate, select I Have Read And Agree To These Terms And Conditions, click Accept, click Browse, and click Upload to upload the earlier created CSR file. Click Download when the certificate is created.

c. Copy the downloaded `MDM_ Microsoft Corporation_Certificate.pem` file and upload the APNs certificate to Windows Intune by browsing to the file and clicking Next (in the wizard) or Apply in the properties of the Windows Intune subscription.

Windows To support the enrollment of Windows RT, Windows RT 8.1, and Windows 8.1, you need to add code-signing certificates and sideloading keys to allow the installation of native apps. Browse to a code-signing certificate, which you can acquire from Symantec, DigiCert, or any other certification authority you can access.

Windows Phone To be able to manage your Windows Phone 8 devices you need to specify the application enrollment token that can be created using your Symantec Enterprise Mobile Code Signing Certificate; you can also install a PFX of the certificate. Also configure an application package (`*.xap`) containing a signed company portal app.

If you want to test the Windows Phone–related mobile device management features, you can download and install the support tool for Windows Intune Trial Management of Window Phone 8. By installing this support tool, you have access to a script that creates a trial certificate for your environment. Some test apps are also available. Download the support tool here: `http://www.microsoft.com/en-us/download/details.aspx?id=39079`.

9. Supply the company contact information, as shown on Figure 16.38, and click Next.

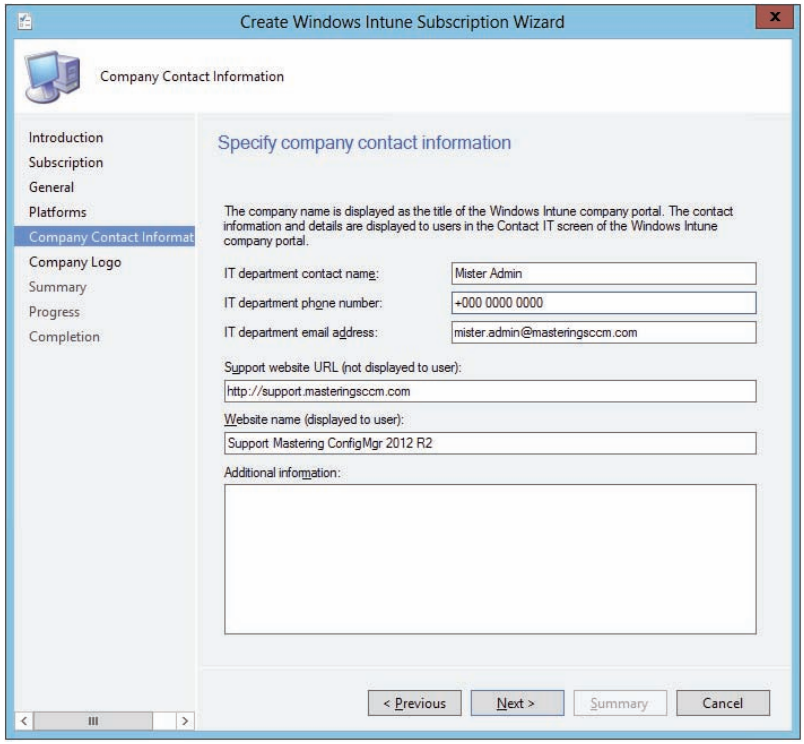


FIGURE 16.38
Company Contact Information page

10. If you want to customize your company portal with a logo, you can upload two JPEG or PNG files that will appear in the company portal of Windows Intune, as shown in Figure 16.39. Click Next after uploading the logos.

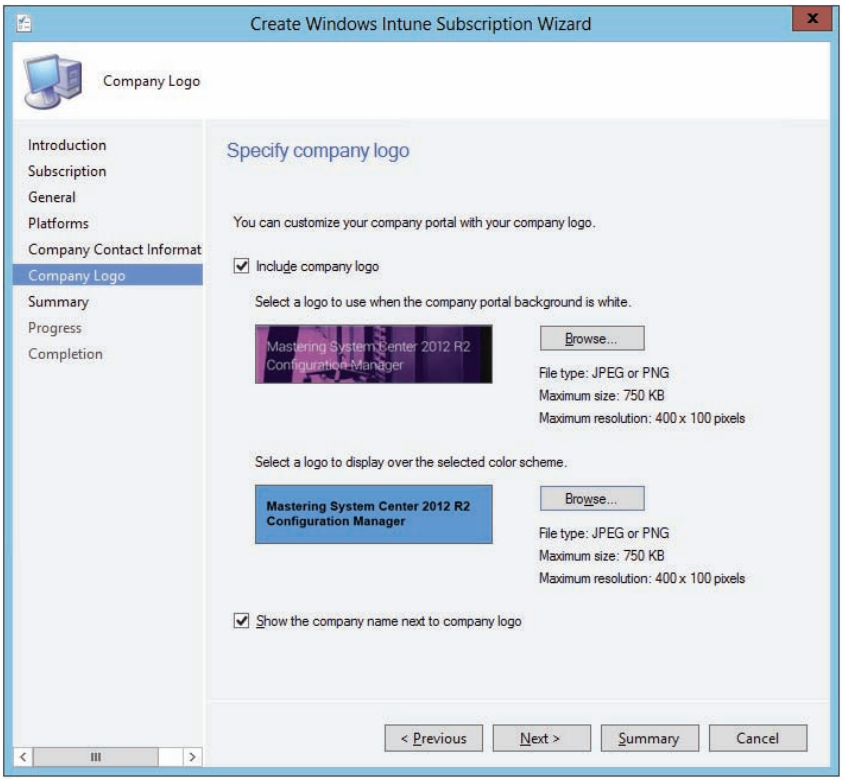


FIGURE 16.39 Company Logo page

11. Review the summary and click Next. Click Close when the configuration is finished.

The last step in configuring the Windows Intune connector is installing the Windows Intune connector itself. In a hierarchy the Windows Intune connector can only be installed on the CAS site server.

12. Open the Configuration Manager 2012 console, select the Administration workspace, and expand Overview ➢ Site Configuration ➢ Servers And Site System Roles. You will see that a site system server named \\manage.microsoft.com is added, as shown in Figure 16.40. This site server is your distribution point within Windows Intune.

13. Select the top-most site server in the hierarchy, and click Add Site System Roles located on the Home tab of the ribbon.

14. Click Next on the General page, and click Next on the Proxy page.

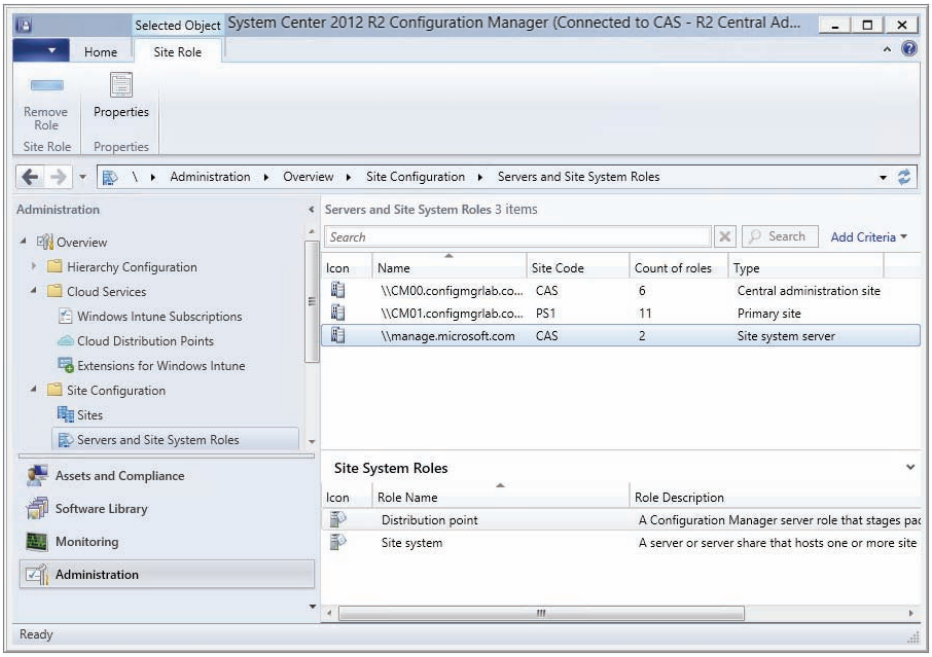


Figure 16.40
A distribution point in Windows Intune is added.

15. Select the Windows Intune connector site role and click Next; review the summary and click Next.
16. Review the results, and click Close once the installation is completed.

Enrolling Mobile Devices

After the prerequisites for the Windows Intune connector are in place and the Windows Intune connector and the supported platforms are configured, you need to enroll your devices. Enrolling devices is done by the users themselves. Each operating system requires different steps.

Android

To enroll an Android device, follow these steps:

1. Go to the Google Play App Store, and search for the Windows Intune Company Portal.
2. Select the Windows Intune Company Portal, and click Install to start the installation. Click Accept to acknowledge that the Windows Intune Company Portal is able to access your storage, information about installed applications, phone calls, and network communication.

3. After the installation is finished, click Open, as shown in Figure 16.41. Next, you need to add your device to Windows Intune and Configuration Manager before you can use the company portal to install company-owned apps. Click Add This Device.

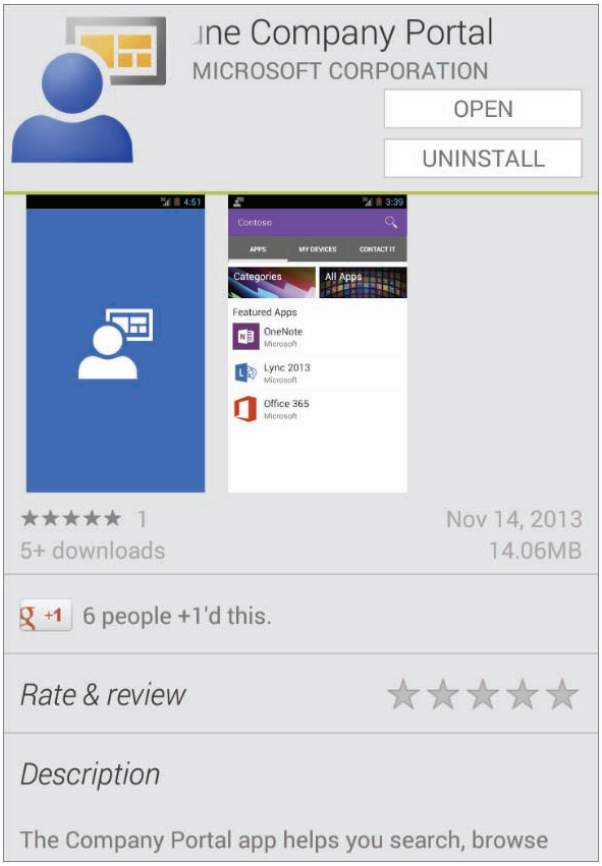


FIGURE 16.41
Open the Windows Intune Company Portal.

4. Next, you need to log on with your Windows Intune account that is allowed to enroll mobile devices. Click Sign In after supplying your Windows Intune credentials.
5. As part of the enrollment process you will be asked to activate the device administrator. This means that the Company Portal will be getting the device administrator permissions to perform the following actions:
   - Erase all data (when executing a Remote Device Wipe)
   - Change the screen-unlock password
   - Set password rules
   - Monitor screen-unlock attempts

- Lock the screen
- Set lock-screen password expiration
- Set storage encryption
- Disable cameras
- Disable features in keyguard.

Click Activate.

6. After activation, the mobile device will be added to the Windows Intune Company Portal, and you will be able to use the portal to install your applications.

iOS

Enrolling an iOS device can be done in two different ways: via the Windows Intune Company Portal and via the Windows Intune Management website.

Let's first look at the process of enrolling the iOS device via the Windows Intune Company Portal. Enrolling is done by following these steps:

1. Search in the Apple App Store for the Windows Intune Company Portal app, and install the app.
2. Click Open to open the Company Portal app, and log on with your Windows Intune user account.
3. Click your device's name in the My Devices section of the Company Portal, as shown in Figure 16.42, and click Add Device. This will start the enrollment process.
4. Click Add on the next screen, which gives you information about allowing your company to manage your device.
5. In the Install Profile dialog, click Install and Install Now.
6. In the Mobile Device Management dialog, click Install.
7. Click Done once the enrollment process is finished.

You can enroll an iOS device via the management portal by following these steps:

1. On your iOS device, start your default web browser and browse to `https://m.manage.microsoft.com`. Supply your Windows Intune—enabled account and password, and click Sign In.
2. On the Company Apps page, click Install. Next, an Install Profile page will appear; here you need to install the Management Profile from manage.microsoft.com by clicking Install.
3. In the Install Profile dialog, click Install Now.
4. Next a warning will be shown stating that installing this profile will allow the administration to remotely manage your mobile device. Click Install.
5. Click Done once the Management Profile is installed.



FIGURE 16.42
Selecting your device to start the enrollment process

Windows Phone 8

In Windows Phone 8 you can enroll your device without installing an app or browsing to a website of Windows Intune. To enroll your Windows Phone 8 device, follow these steps:

1. Choose Settings ➢ Company Apps and click Add Account.
2. Supply your email address and password, and click Sign In.
3. Click Done when the company account is successfully added; leave Install Company App Or Hub selected. After clicking Done, you may receive a message that company policies can be applied. Your company can offer policies, certificates, and apps that help you connect to your business or secure your mobile device, as shown in Figure 16.43.

Windows RT, Windows 8.1

Windows RT and Windows 8.1 devices can also be managed without joining them to your domain. An option called Workplace Join allows you to enroll your device in Configuration Manager 2012 R2. After enrolling your device you can receive apps and settings from Configuration Manager 2012 R2. Joining your Windows RT or Windows 8.1 device can be done as follows:



Figure 16.43
Windows Phone device enrolled

1. In Windows, choose Settings ➢ Network ➢ Workplace.
2. Supply your user ID and click Turn On.
3. Select I Agree and click Turn On, as shown in Figure 16.44.

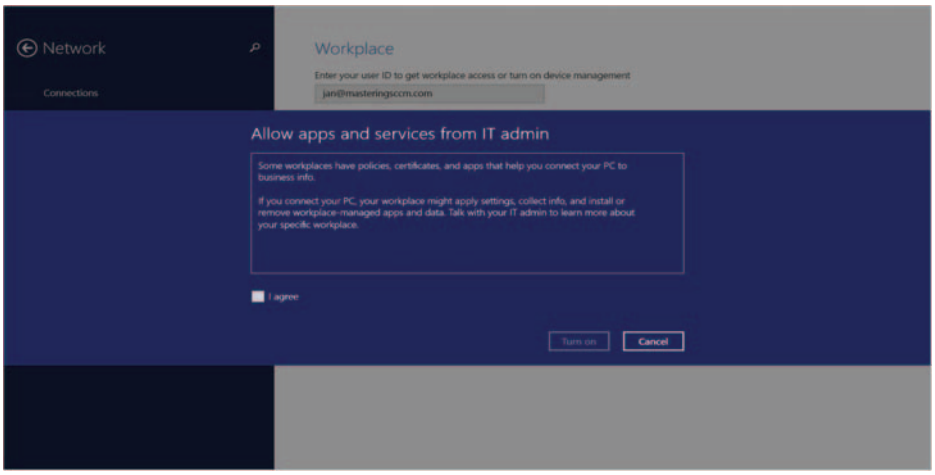


Figure 16.44
Turn on Workplace Join.

After all devices are enrolled, they will show up in the Configuration Manager 2012 R2 console, as shown in Figure 16.45.

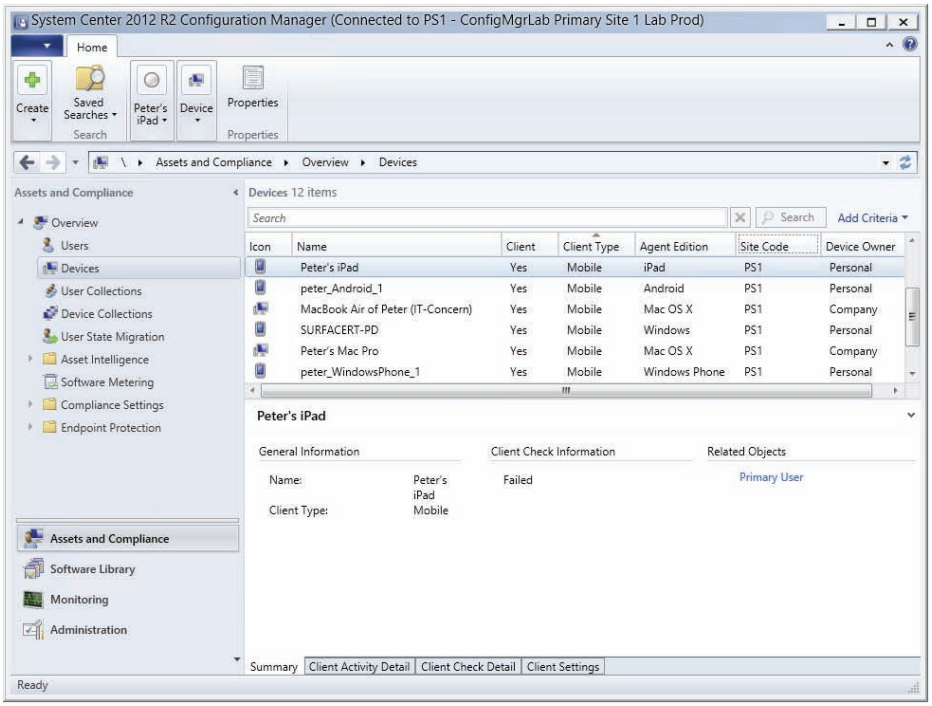


FIGURE 16.45 Enrolled devices in Configuration Manager

Managing Mobile Devices

After enrolling the devices, you can manage your mobile devices via Configuration Manager 2012 R2.

COMPLETE FEATURE LIST OF MANAGING MOBILE DEVICES

Since the feature set of Windows Intune is changing quickly and features are added on the spot, be sure to check the latest version of the TechNet documentation for the latest status:

`http://technet.microsoft.com/en-us/library/dn376523.aspx`

Device Settings Management

Settings management options are available for depth devices in addition to the standard client operations. You configure these settings through Compliance Settings. Configuring settings for mobile devices requires creating one or more configuration items and then delivering them to the mobile devices by associating them with configuration baselines, which are then assigned to a given collection. Also, you can create Company Resource Access Profiles and deploy them to

your mobile devices. Since the number of configuration items and baselines needed depends on individual configurations, the example will use a unified approach where a single configuration item and baseline are used for all devices:

1. Start creating the configuration item by selecting Compliance Settings ➢ Configuration Items.
2. Right-click Configuration Items and select Create Configuration Item.
3. On the General page of the Create Configuration Item Wizard, supply a name and description and then specify that the configuration item is targeted for a mobile device.
4. Optionally, select any categories that should be used for this configuration item. Click Next.
5. On the Mobile Device Settings page, determine which settings should be managed by this configuration item.

   For the example, select all settings and choose to configure additional settings, as shown in Figure 16.46. This will allow you to review all potential settings that might be enforced on a device. Click Next.

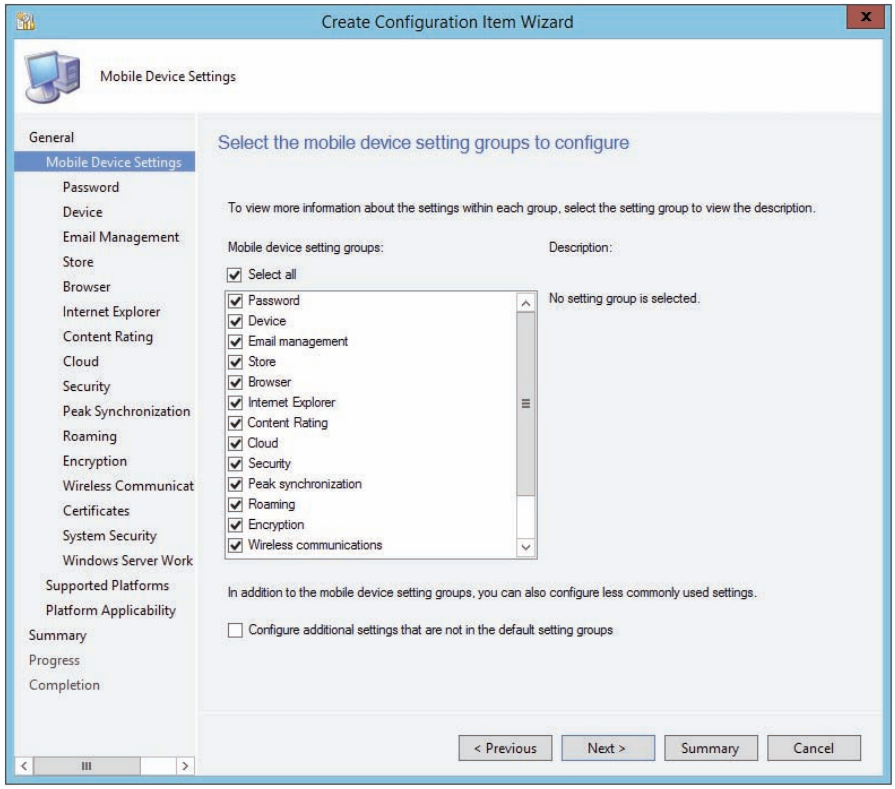


Figure 16.46
Create Configuration Item Wizard—Mobile Device Settings page

Settings vs. Device Capability

Not all devices are capable of implementing all settings. It's fine to configure a setting in general, but the settings will be implemented only on capable devices.

6. After selecting the additional settings that will be defined by this configuration item, click Next.
7. Configure the appropriate mobile device password options.

   The password settings are shown in Figure 16.47. Password settings are not configured by default.

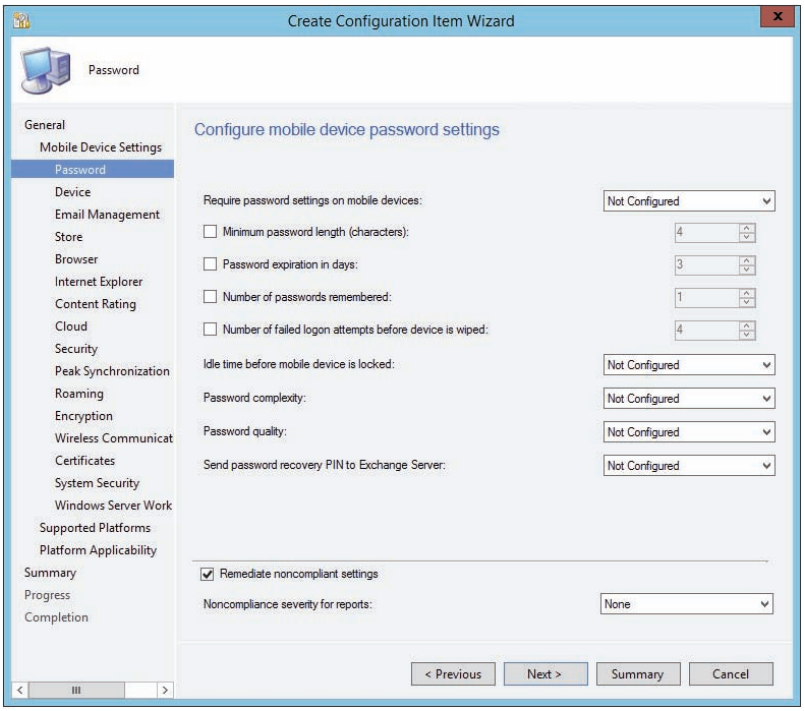


Figure 16.47 Create Configuration Item Wizard—Password page

Require Password Settings On Mobile Devices This option allows administrators to determine whether password settings should be enforced. Assuming this option is enabled, a few specific password configurations are possible:

- Minimum Password Length (Characters): This option allows administrators to specify the minimum number of characters that should be supplied as part of the password.
- Password Expiration In Days: This option allows administrators to specify the number of days that are allowed to elapse before requiring a password change.
- Number Of Passwords Remembered: This option allows administrators to configure how many passwords are retained. This setting is useful to prevent the reuse of passwords.
- Number Of Failed Logon Attempts Before Device Is Wiped: This option allows administrators to specify how many incorrect passwords can be supplied before the device is automatically wiped.

Idle Time Before Mobile Device Is Locked This option, not enabled by default, allows administrators control over how long a device might be left unlocked when idle.

Password Complexity This option allows administrators to specify the required password complexity level, in this case allowing either a PIN or a strong password.

Password Quality This option allows you to configure how the password must be built, for instance, if it must be at least Numeric, Alphabetic, or Alphanumeric. You can also configure it as Required, Low Security Biometric, or Alphanumeric With Symbols.

Send Password Recovery PIN To Exchange Server This option allows administrators to configure where the password recovery PIN is stored on the Exchange server.

Device Compliance Remediation

If a device is not compliant with all required settings, it will be updated to the required state by default as a result of selecting Remediate Noncompliant Settings on the Password page. When device settings are remediated, it is possible to configure that a noncompliance indication will be logged in reports. This is disabled by default.

8. After all password options are configured, click Next.
9. Configure device settings for the device on the Device page, shown in Figure 16.48.

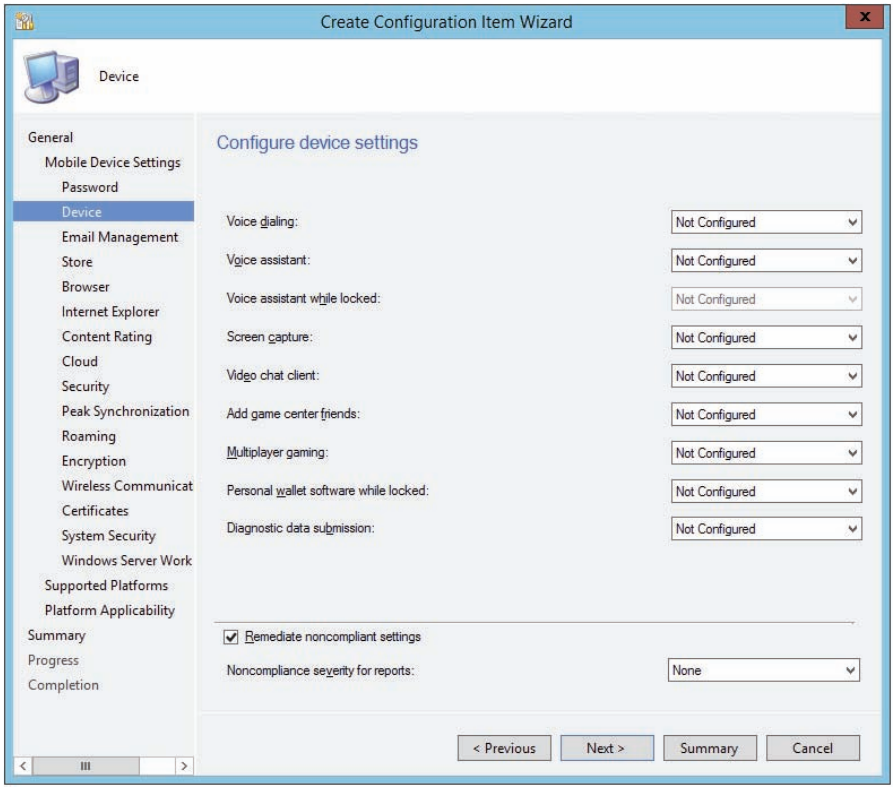


FIGURE 16.48
Create Configuration Item Wizard—Configure Device Settings

Voice Dialing This option allows administrators to define whether voice dialing is allowed. It can be configured as Allowed or Prohibited.

Voice Assistant This option allows administrators to define whether the voice assistant is allowed. It can be configured as Allowed or Prohibited.

Voice Assistant While Locked This option allows administrators to define whether the voice assistant is allowed while locked. It can be configured as Allowed or Prohibited.

Screen Capture This option allows administrators to define whether screen capture is enabled or not. It can be configured as Enabled or Disabled.

Video Chat Client This option allows administrators to define whether the video chat client is enabled or not. It can be configured as Enabled or Disabled.

Add Game Center Friends This option allows administrators to define whether adding game center friends is allowed. It can be configured as Allowed or Prohibited.

Multiplayer Gaming This option allows administrators to define whether multiplayer gaming is allowed. It can be configured as Allowed or Prohibited.

Personal Wallet Software While Locked This option allows administrators to define whether personal wallet software is allowed while locked. It can be configured as Allowed or Prohibited.

Diagnostic Data Submission This option allows administrators to define whether diagnostic data submission is enabled or not. It can be configured as Enabled or Disabled.

10. Click Next to configure email options for the device in the Email Management settings, shown in Figure 16.49.

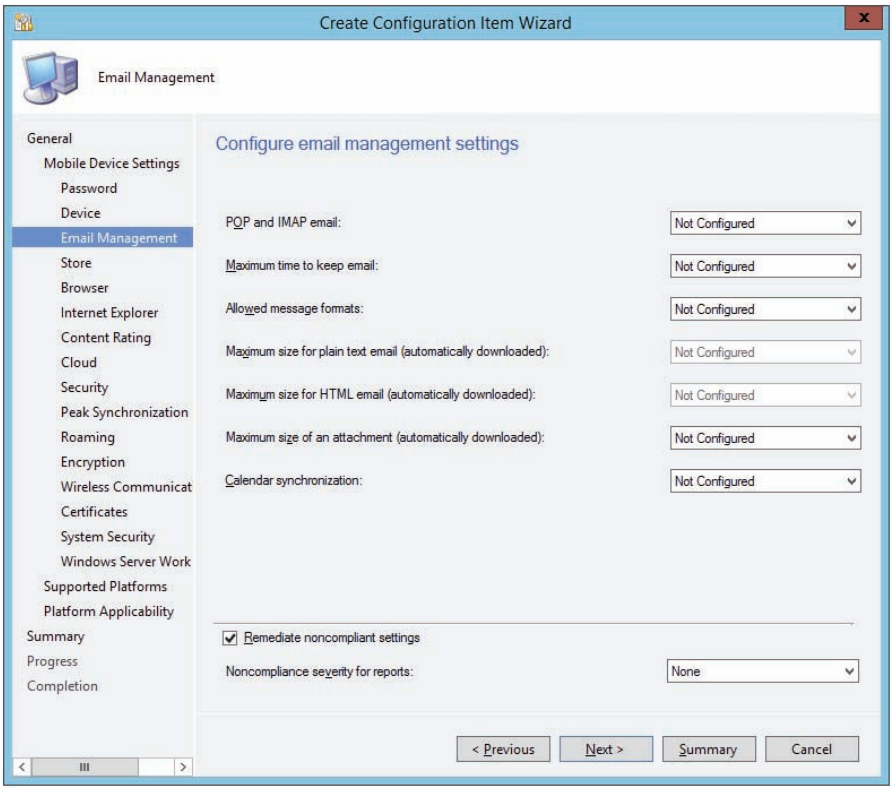


FIGURE 16.49
Create Configuration Item Wizard—Email Management page

PDP And IMAP Email This option allows administrators to define whether PDP and IMAP email are allowed. This is not an either/or setting; either both are allowed or both are prohibited.

Maximum Time To Keep Email This option allows administrators to specify how long email should be retained on the device.

Allowed Message Formats This option allows administrators to specify the format allowed for email, either plain text only or both plain text and HTML. If this option is configured, up to two additional options become available for configuration.

Maximum Size For Plain Text Email (Automatically Downloaded) This option allows administrators to define the size of a plain text email that is allowed to be automatically downloaded to the device. Incremental sizes are configurable up to allowing the entire email to be downloaded.

Maximum Size For HTML Email (Automatically Downloaded) This option allows administrators to define the size of an HTML email that is allowed to be automatically downloaded to the device. Incremental sizes are configurable up to allowing the entire email to be downloaded.

Maximum Size Of An Attachment (Automatically Downloaded) This option allows administrators to define the size of an attachment that is allowed to be automatically downloaded to the device. Incremental sizes are configurable up to allowing the entire email to be downloaded.

Calendar Synchronization This option allows administrators to specify whether calendar synchronization to the device is allowed.

11. After all email options are configured, click Next.
12. Configure the store settings, shown in Figure 16.50.

    Application Store This option allows administrators to specify whether accessing and using the application store of the device is allowed.

    Enter A Password To Access The Application Store This option allows administrators to specify whether a user must enter a password when accessing an application store.

    In-App Purchases This option allows administrators to specify whether in-app purchases are allowed.

13. After configuring the application store settings, click Next.
14. Configure the browser settings, shown in Figure 16.51.

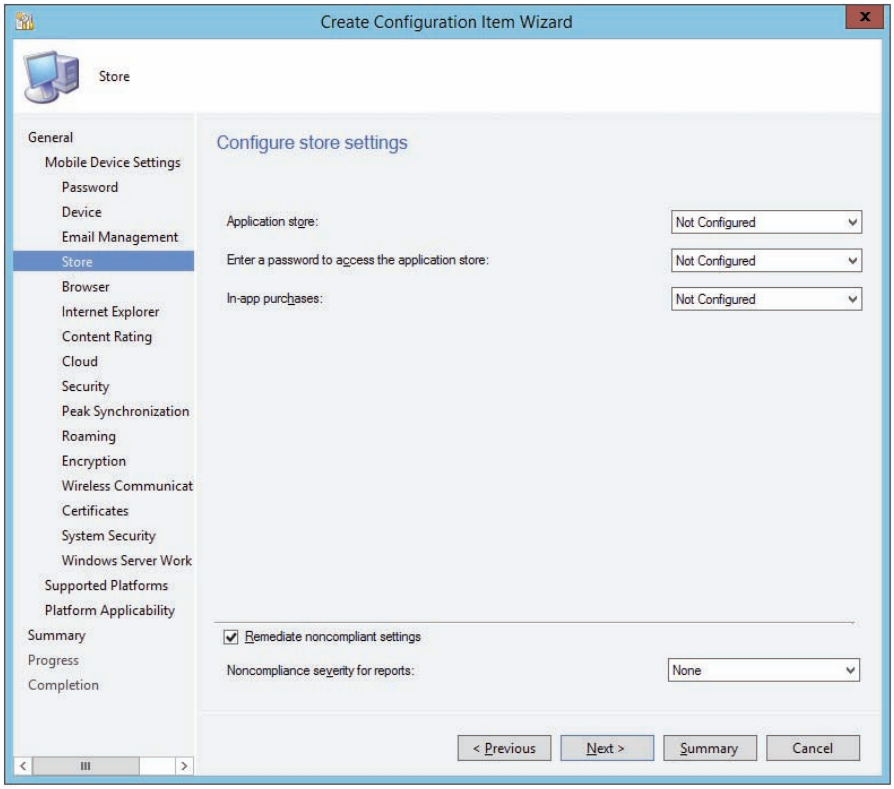


FIGURE 16.50 Create Configuration Item Wizard—Store page

Default Browser Configure if a user is allowed to change the default browser or not.

Autofill Configure if the browser is allowed to use autofill or not.

Active Scripting Configure if the browser is allowed to use active scripting or not.

Plug-ins Configure if the browser is allowed to use plug-ins or not.

Pop-up Blocker Configure if the browser is allowed to use the pop-up blocker or not.

Cookies Configure if the browser is allowed to accept cookies or not.

Fraud Warning Configure if fraud warning in the browser is enabled or not.

15. After configuring the browser settings, click Next.
16. For the Windows-based mobile devices you can configure Internet Explorer settings, as shown in Figure 16.52.

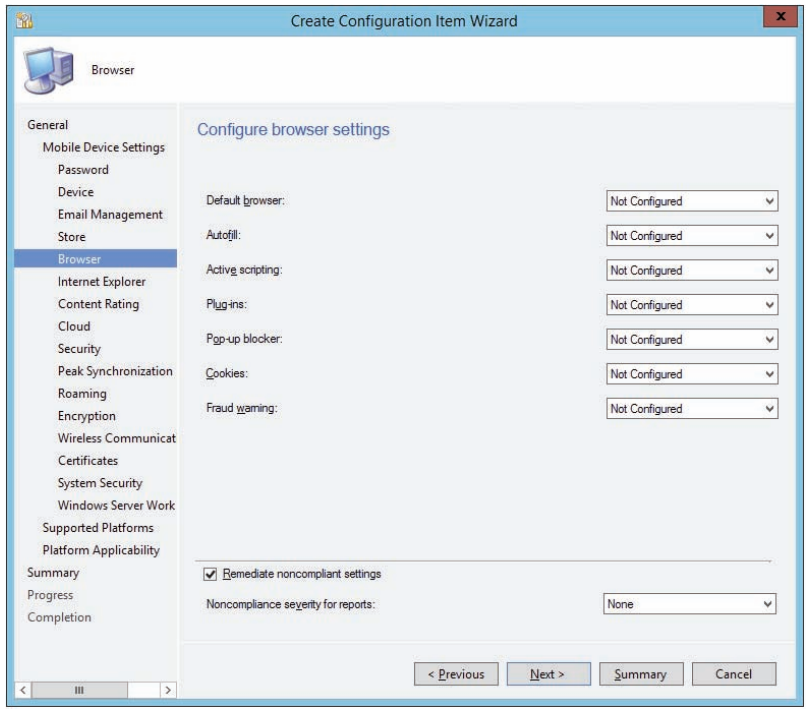


FIGURE 16.51
Create Configuration Item Wizard—Browser page

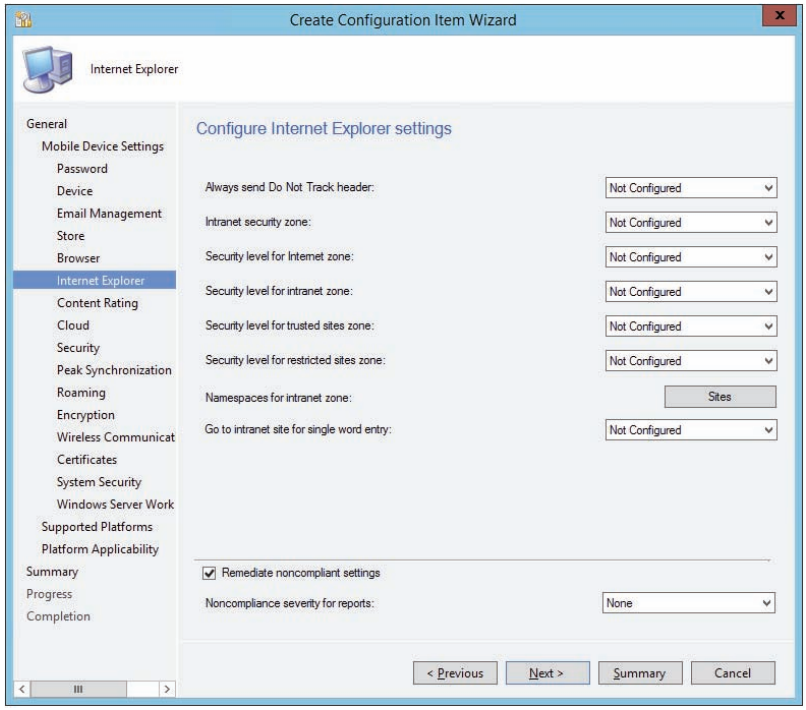


FIGURE 16.52
Create Configuration Item Wizard—Internet Explorer page

Always Send Do Not Track Header Configure whether the Always Send Do Not Track Header option can be enabled or not.

Intranet Security Zone Configure whether the Intranet security zone settings can be changed or not.

Security Level For Internet Zone Configure whether the security level for the Internet zone can be changed or not.

Security Level For Intranet Zone Configure whether the security level for the intranet zone can be changed or not.

Security Level For Trusted Sites Zone Configure whether the security level for the trusted sites zone can be changed or not.

Security Level For Restricted Sites Zone Configure whether the security level for the restricted sites zone can be changed or not.

Namespaces For Intranet Zone Preconfigure the namespaces for your intranet zone or enforce that websites are removed from the intranet zone.

Go To Intranet Site For Single Word Entry Configure whether a user is redirected to an intranet when supplying a single word.

17. Click Next to configure the Content Rating settings, as shown in Figure 16.53. Content ratings apply to iOS devices only.

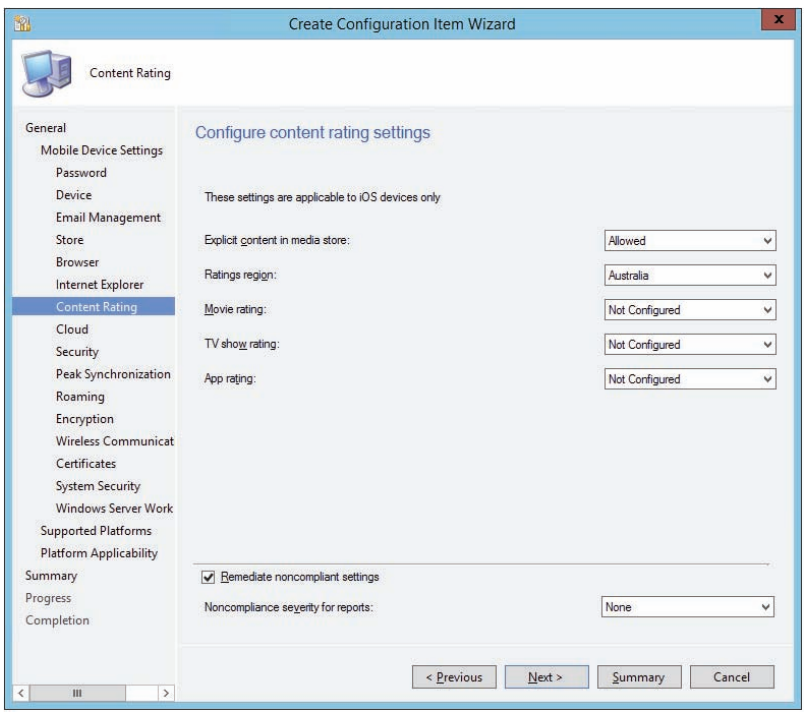


Figure 16.53
Create Configuration Item Wizard—Content Rating page

Explicit Content In Media Store Configure if iOS devices can be restricted to explicit media content in the Apple store.

Ratings Region Configure from which region the content can be acquired; the following regions can be configured: United States, Australia, Canada, Germany, France, Ireland, Japan, New Zealand, and United Kingdom.

Movie Rating Specify the ratings that movies downloaded from the Apple store can have. Options are Don't Allow, G, PG, M, MA15+, R18+, and Allow All.

TV Show Rating Specify the ratings that TV shows downloaded from the Apple store can have. Options are Don't Allow, P, C, G, PG, M, MA15+, AV15+, and Allow All.

App Rating Specify the ratings that apps downloaded from the Apple store can have. Options are Don't Allow, 4+, 9+, 12+, 17+, and Allow All.

18. Click Next to configure the cloud settings, as shown in Figure 16.54.

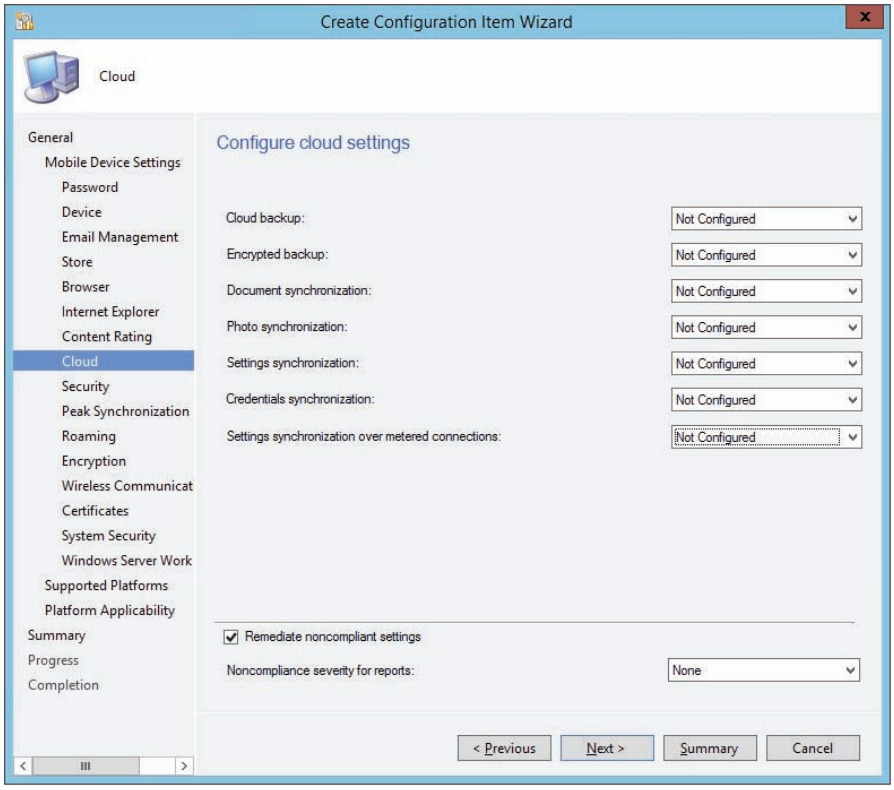


FIGURE 16.54 Create Configuration Item Wizard—Cloud page

Cloud Backup Configure whether the mobile device can back up the device to a cloud backup service or not.

Encrypted Backup Configure whether a backup of device can be encrypted or not.

Document Synchronization Configure whether documents on the mobile devices may be synchronized to a cloud service like SkyDrive or iCloud on the Internet or not.

Photo Synchronization Configure whether photos on the mobile devices may be synchronized to a cloud service like SkyDrive or iCloud on the Internet or not.

Settings Synchronization Configure whether settings on the mobile devices may be synchronized to a cloud service like SkyDrive or iCloud on the Internet or not.

Credentials Synchronization Configure whether credentials on the mobile devices may be synchronized to a cloud service like SkyDrive or iCloud on the Internet or not.

Settings Synchronization Over Metered Connections Configure whether synchronizations over metered connections are allowed or not.

19. Configure the security options for the device. The security management settings are shown in Figure 16.55.

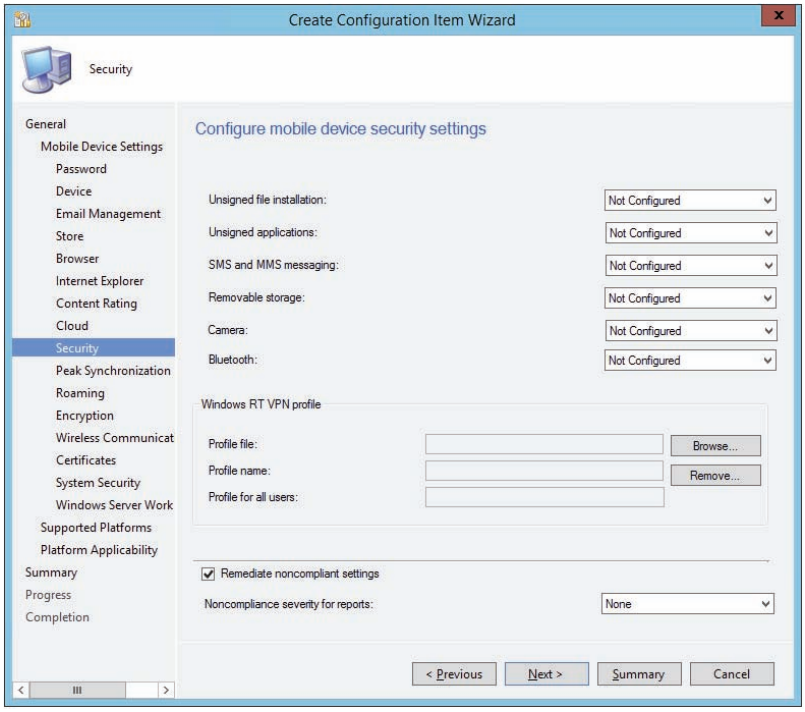


Figure 16.55 Create Configuration Item Wizard—Security page

Unsigned File Installation This option allows administrators to specify whether the installation of unsigned files is allowed or not allowed. If they are allowed, administrators then choose what parties are allowed this right. Available options are Mobile Operator, Manager, User Authenticated, IT Administrator, User Unauthenticated, and Trusted Provisioning Server.

Unsigned Applications This option allows administrators to specify whether the installation of unsigned applications is allowed or prohibited.

SMS And MMS Messaging This option allows administrators to configure whether SMS and MMS messaging are allowed or prohibited on the device.

Removable Storage This option allows administrators to configure whether removable storage is allowed or prohibited on the device.

Camera This option allows administrators to configure whether the camera is allowed or prohibited on the device.

Bluetooth This option allows administrators to configure whether Bluetooth is allowed or prohibited on the device.

Windows RT VPN Profile Deploy a VPN profile for a Windows RT device and define if the profile is available to all users or not.

20. After all security options are configured, click Next.
21. Configure the synchronization options for the device in the Peak Synchronization settings, shown in Figure 16.56.

    Specify Peak Time This option allows administrators to define the specific time considered to be peak on devices.

    Peak Synchronization Frequency This option allows administrators to specify how often the device will synchronize during the defined peak time.

    Off-Peak Synchronization Frequency This option allows administrators to specify how often the device will synchronize outside the defined peak time.

22. After all peak synchronization options are configured, click Next.
23. Configure the roaming options for the device in the Roaming settings, shown in Figure 16.57.

    Mobile Device Management While Roaming This option allows administrators to configure whether a device should be actively managed when roaming.

    Software Download While Roaming This option allows administrators to specify whether software downloads should be allowed when a device is roaming.

    Email Download While Roaming This option allows administrators to control whether email is downloaded while a device is roaming.

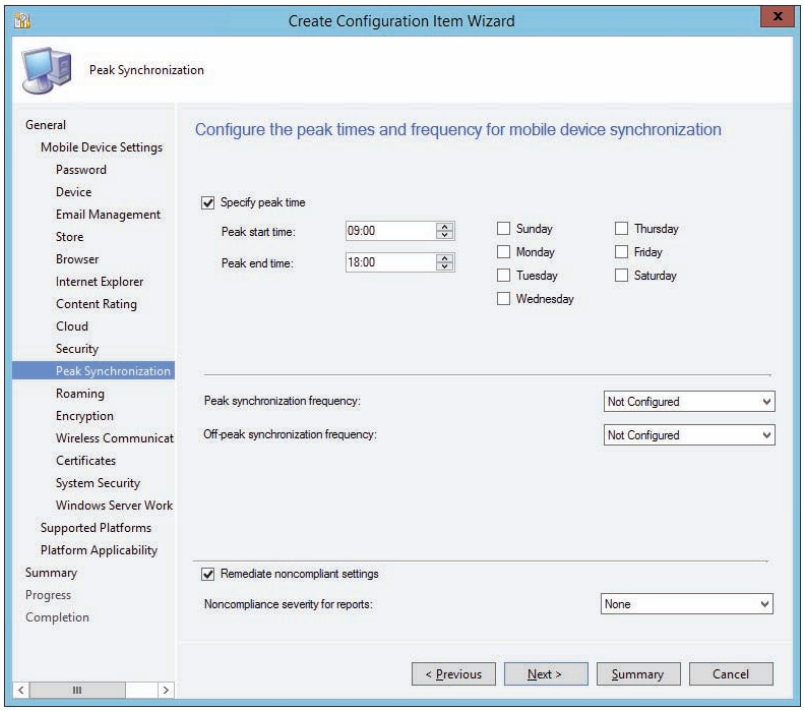


Figure 16.56
Create Configuration Item Wizard—Peak Synchronization page

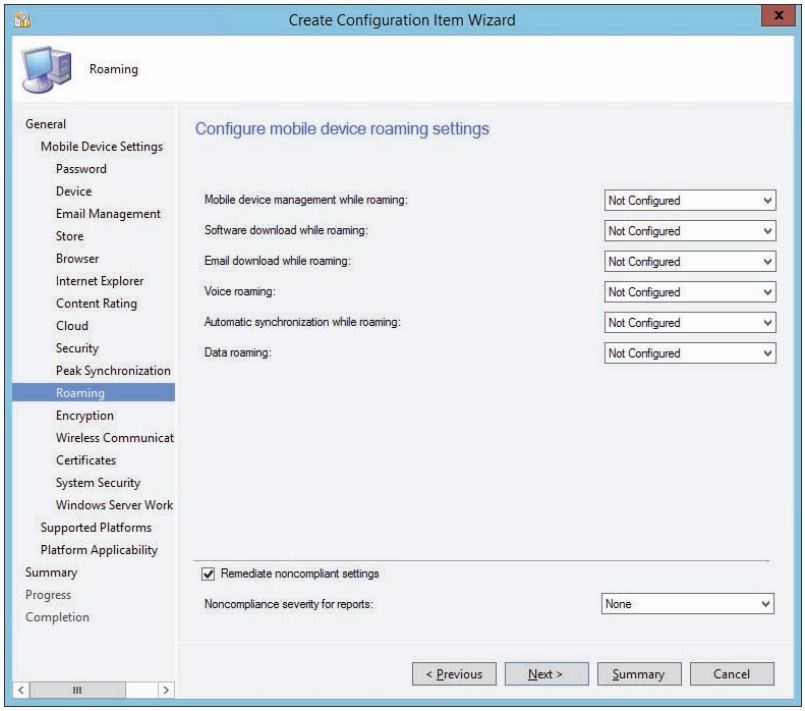


Figure 16.57
Create Configuration Item Wizard—Roaming page

Voice Roaming This option allows administrators to control whether voice roaming is allowed.

Automatic Synchronization While Roaming This option allows administrators to control whether automatic synchronization is allowed while a device is roaming.

Data Roaming This option allows administrators to control whether data usage is allowed while a device is roaming.

24. After all the roaming options are configured, click Next.
25. Configure the encryption options for devices in the Encryption settings, shown in Figure 16.58.

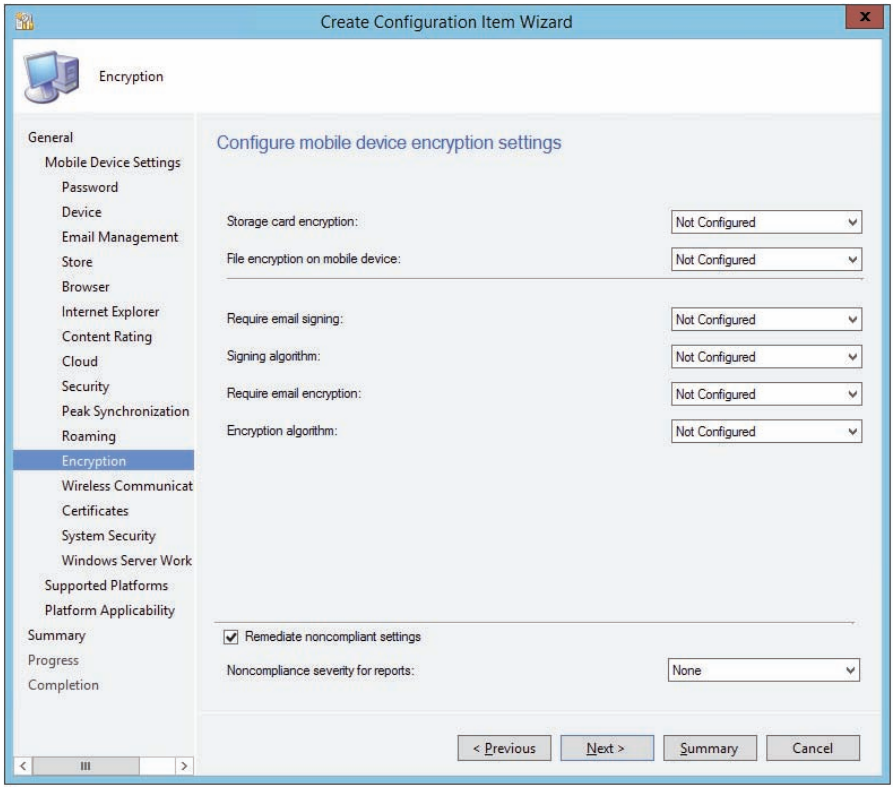


FIGURE 16.58 Create Configuration Item Wizard—Encryption page

Storage Card Encryption This option allows administrators to specify whether encryption is on or off for a device's storage card.

File Encryption On Mobile Device This option allows administrators to configure whether file encryption is on or off for a device.

Require Email Signing/Signing Algorithm This option allows administrators to specify whether email signing is enabled or disabled. If email signing is enabled, the Signing Algorithm option allows administrators to specify whether SHA, MD5, or the default signing algorithm should be used.

Require Email Encryption/Encryption Algorithm This option allows administrators to configure whether email encryption is on or off for a device. If email encryption is enabled, the Encryption Algorithm option allows administrators to specify which encryption algorithm should be used. Available choices are Triple DES, DES, RC2 128-bit, RC2 64-bit, RC2 40-bit, and the default algorithm.

26. After all encryption options are configured, click Next.

27. Configure the wireless communication options for devices in the Wireless Communication settings, shown in Figure 16.59.

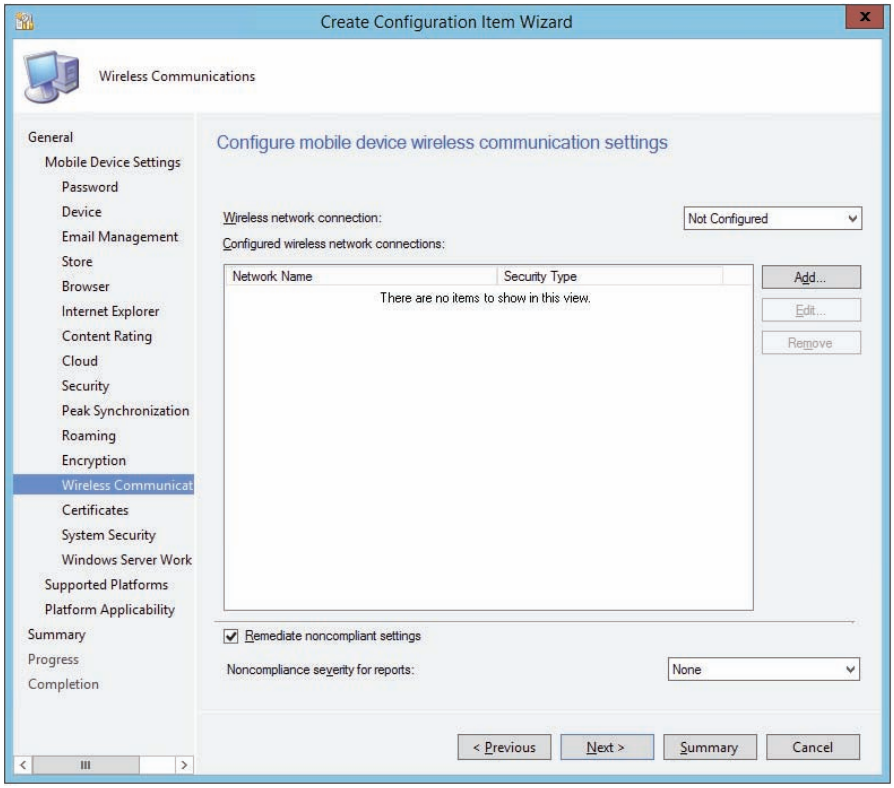


FIGURE 16.59
Create Configuration Item Wizard—Wireless Communications page

28. Configure whether wireless network connections are allowed or prohibited on the device.

If they are allowed, administrators can click the Add button to specify one or more networks and the associated network configuration. Available network configuration options include Proxy, 802.1X, Authentication, Data Encryption, and more. A blank Wireless Network Connection configuration page is shown in Figure 16.60.

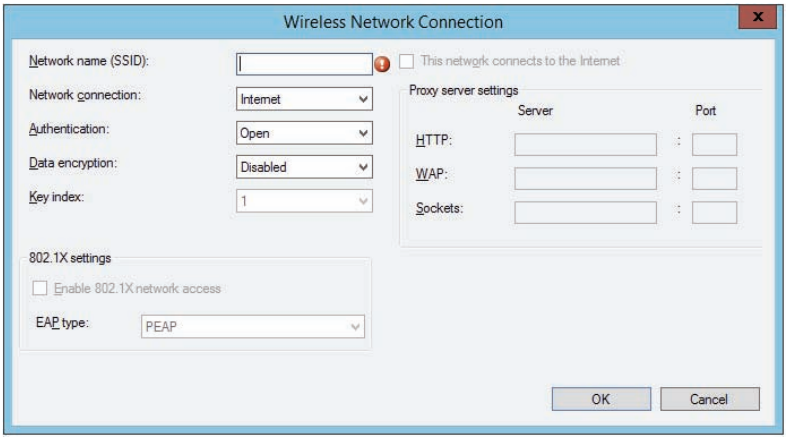


FIGURE 16.60
Wireless Network Connection page

29. After all wireless network connection options are configured, click Next.

30. Configure the certificate options for devices in the Certificates settings, shown in Figure 16.61.

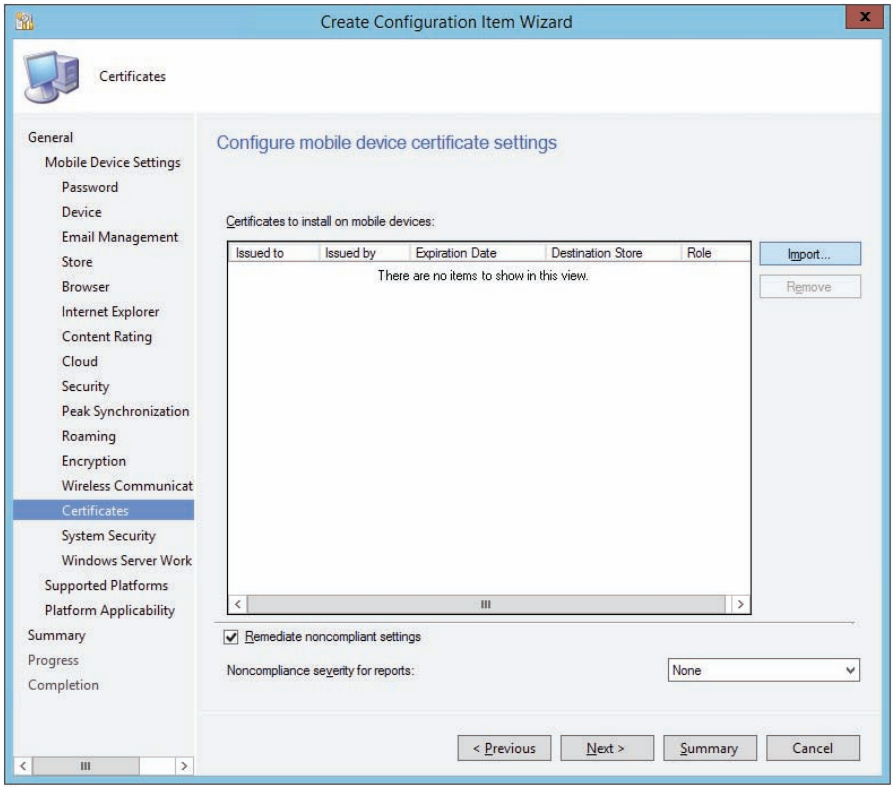
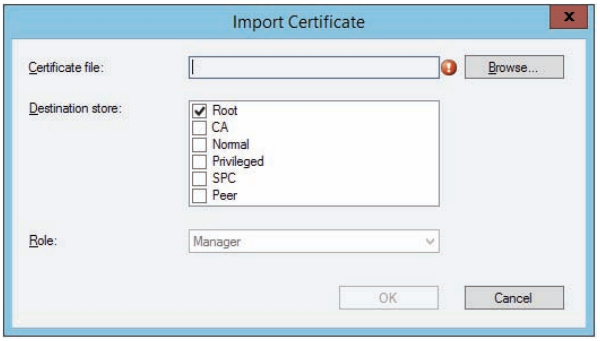


FIGURE 16.61
Create Configuration Item Wizard—Certificates page

The Certificates To Install On Mobile Devices option allows administrators to specify certificates that should be installed on mobile devices. Clicking the Import button brings up the Import Certificate dialog, shown in Figure 16.62, which allows certificates to be imported from the filesystem and allows administrators to specify in which certificate store the certificate should be placed on the device.

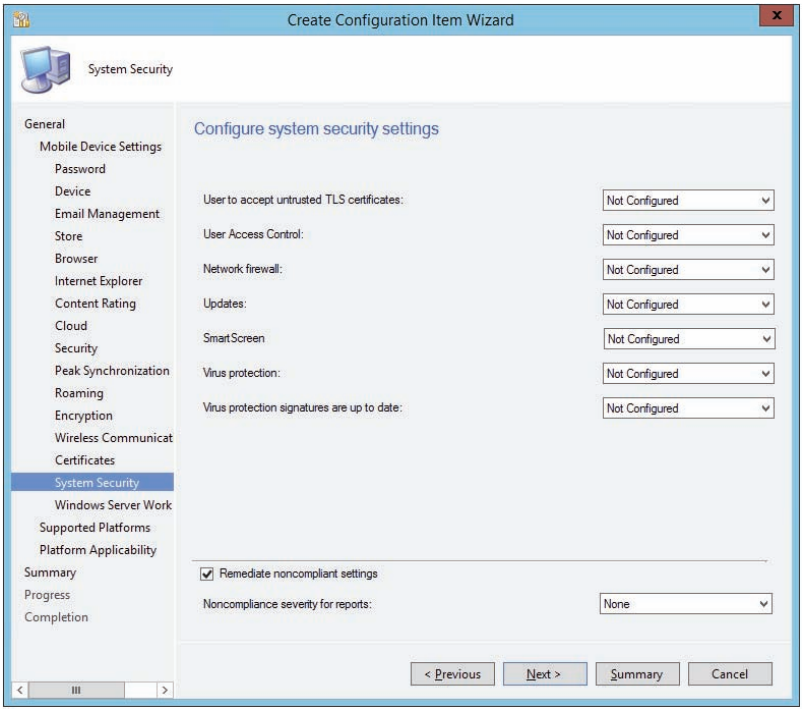
FIGURE 16.62
Import Certificate dialog



31. After all certificate options are configured, click Next.

32. Configure extra security settings on the System Security page, shown in Figure 16.63. This system security will apply to Windows-based devices.

FIGURE 16.63
Create Configuration Item Wizard—System Security page



User To Accept Untrusted TLS Certificates This option allows administrators to configure whether a user is allowed to accept untrusted TLS certificates.

User Access Control This option allows administrators to configure how User Access Control is enabled and how it notifies them of changes to the operating system of a device.

Network Firewall This option allows administrators to configure whether the firewall is required or not.

Updates This option allows administrators to configure whether updates are installed automatically or not.

SmartScreen This option allows administrators to configure whether SmartScreen in Internet Explorer is enabled or not.

Virus Protection This option allows administrators to configure whether virus protection is required for a device.

Virus Protection Signatures Are Up To Date This option allows administrators to configure whether up-to-date virus protection signatures are required or not.

33. Once the security settings are configured, click Next to configure Windows Server Work Folder settings, as shown in Figure 16.64.

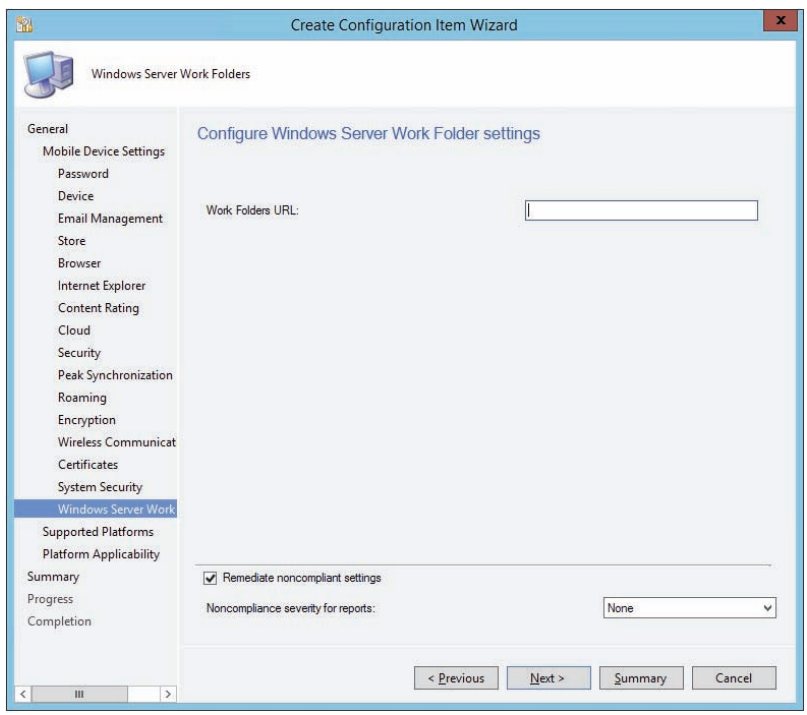


FIGURE 16.64 Create Configuration Item Wizard—Windows Server Work Folders page

34. Click Next to configure the Supported Platforms page, shown in Figure 16.65, specify which platforms should be targeted with the configurations just defined, and click Next.

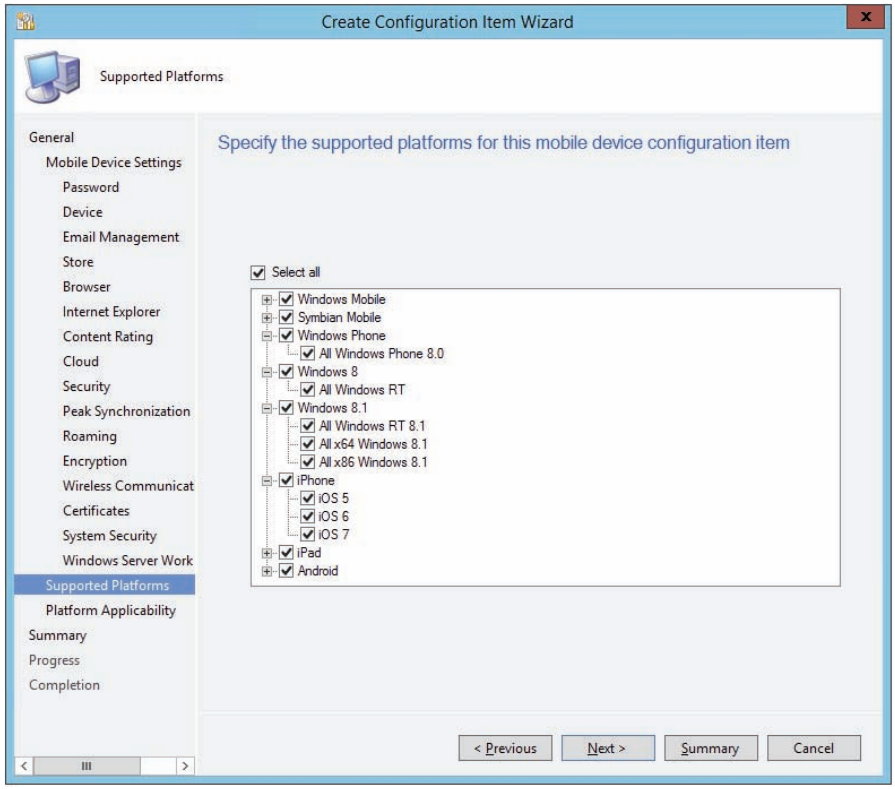


FIGURE 16.65
Create Configuration Item Wizard—Supported Platforms page

As already mentioned, not all settings apply to all device types. The Platform Applicability page of the wizard, shown in Figure 16.66, displays any settings that have been chosen but are not supported by a selected target platform. There is no configuration available here.

35. From here, simply complete the wizard to save the configuration item.

Defining the configuration item is not sufficient. Implementing the configuration item requires attaching it to a baseline and assigning that baseline to a collection. This is a general task for compliance setting management and is discussed in Chapter 14, "Compliance Settings."

Now that we have looked at the configuration settings, we also have to look at the profiles that can be managed from Configuration Manager 2012 R2. You can use Configuration Manager to configure certificate, VPN, and Wi-Fi profiles for devices that are managed via Configuration Manager 2012 R2.

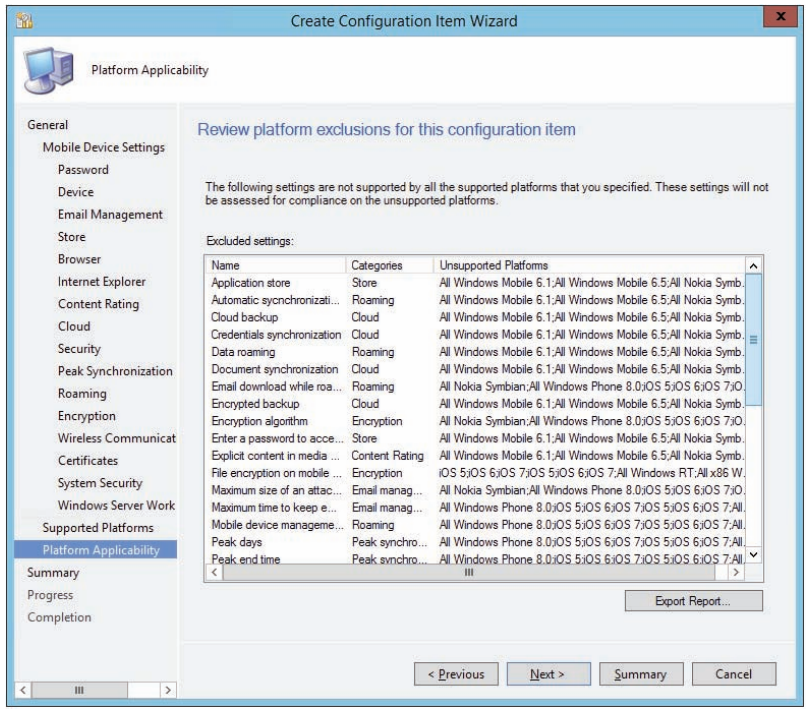


Figure 16.66
Create Configuration Item Wizard—Platform Applicability page

1. Start configuring the configuration item by selecting Compliance Settings ➢ Company Resource Access.
2. Click Certificate Profiles ➢ Create Certificate Profile in the Home tab of the ribbon.
3. Supply a name and specify the type of certificate profile that you want to create. This allows you to deploy a trusted CA certificate or use the Simple Certificate Enrollment Protocol (SCEP) settings. Before you can create a profile for a SCEP, you need to first add a Trusted CA certificate. Select the option Trusted CA Certificate and click Next.
4. Select a CA certificate file by clicking Import, and select the destination store before clicking Next, as shown in Figure 16.67. The certificate thumbprint will be imported from the certificate file and displayed.
5. Click Next and select the platforms that will be provisioned with this new certificate profile. Click Next.
6. Review the Summary page and click Next. Click Close when the certificate profile is created successfully.
7. After the Trusted Root CA certificate profile has been created, you can create a SCEP certificate profile. In a new Create Certificate Profile Wizard, select the option Simple Certificate Enrollment Protocol (SCEP) settings and click Next.

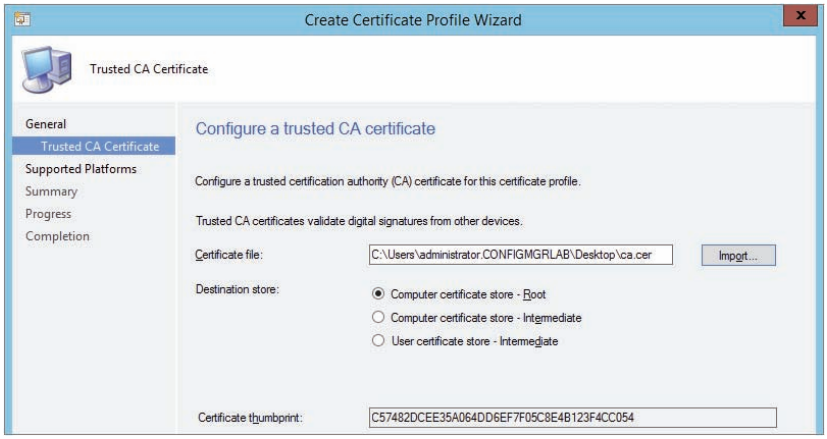


Figure 16.67
Create Certificate Profile Wizard—Trusted CA Certificate page

8. Configure the SCEP certificate enrollment parameters as shown in Figure 16.68, and click Next.

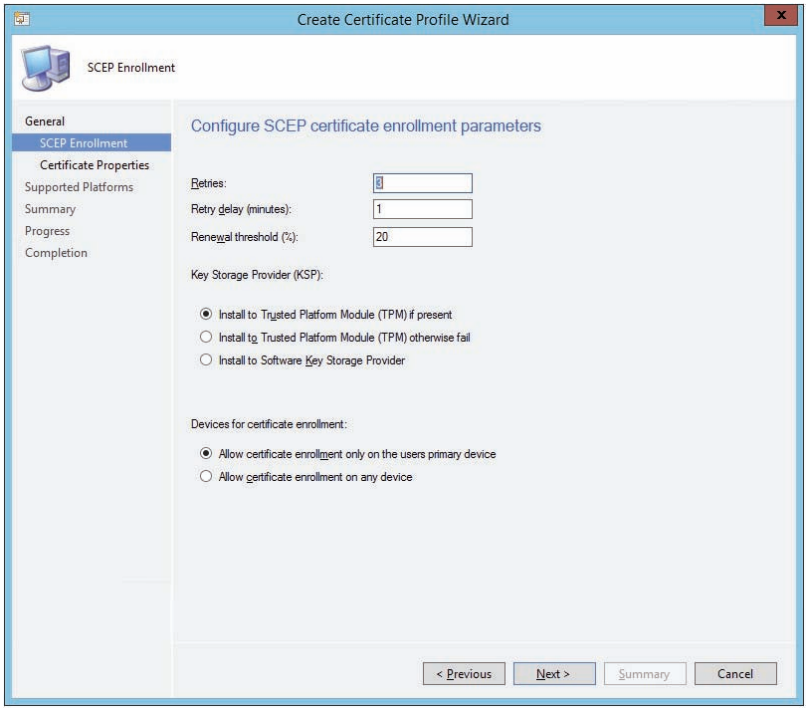


Figure 16.68
Create Certificate Profile Wizard—SCEP Enrollment page

Retries/Retry Delay (Minutes)/Renewal Threshold (%) Configure how often an enrollment retry may take place, with the number of minutes between retries.

Key Storage Provider (KSP) This option allows administrators to configure whether to install to Software Key Storage Provider, Trusted Platform Module (TPM) if present, or fail if TPM is not available.

Devices For Certificate Enrollment This option allows administrators to configure whether the certificate is enrolled by the user on any device or only on the user's primary device.

9. The next step is to configure the certificate properties, as shown in Figure 16.69.

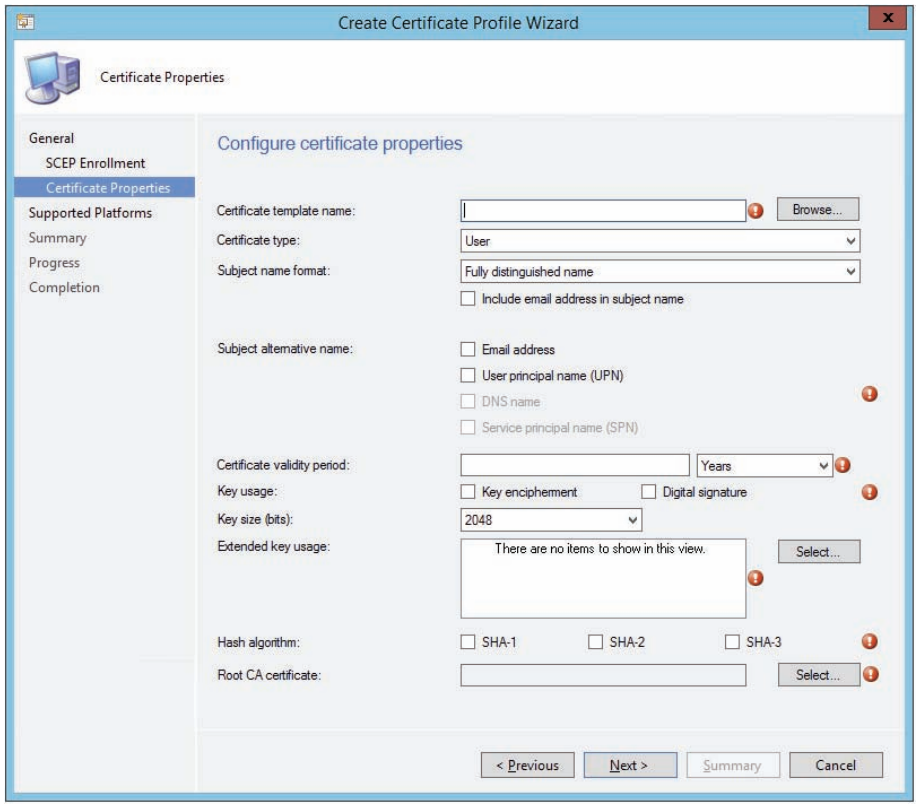


FIGURE 16.69 Create Certificate Profile Wizard—Certificate Properties page

Certificate Template Name Supply a certificate template name by clicking the Browse button. Select the issuing certificate authority and the certificate template name before clicking OK.

Certificate Type Define whether the certificate is a User or Device certificate.

Subject Name Format Depending on whether the certificate is a User or Device certificate, you can supply different name formats. If it is a User certificate, you can enable the Include Email Address In Subject Name option.

Subject Alternative Name Depending on whether the certificate is a User or Device certificate, you can add subject alternative names to the certificate. Alternative names can be an email address, user principal name (UPN), DNS name, or service principal name (SPN).

Certificate Validity Period Configure the validity period of the certificate in days, months, or years, depending on the configured certificate template.

Key Usage If not grayed out (depending on the certificate template), you can enable Key Encipherment and Digital Signature.

Key Size (Bits) If not grayed out (depending on the certificate template), you can configure the key size of the certificates.

Extended Key Usage If not grayed out (depending on the certificate template), you can select the extended key usage options. If grayed out, you will see the options available in the certificate template.

Hash Algorithm Select the SHA-1, SHA-2, or SHA3 hash algorithms that are going to be used.

Root CA Certificate Select the Trusted Root CA certificate profile you created earlier and click OK.

10. Click Next, and select the platforms that will be provisioned with this new certificate profile. Click Next.
11. Review the Summary page, and click Next. Click Close when the SCEP certificate profile is created successfully.

You can deploy the certificate profiles to your test collections before rolling out the profiles to a broader range of mobile devices.

As mentioned earlier, besides certificate profiles, you can use Configuration Manager 2012 R2 to create and deploy VPN profiles. To create a VPN profile, follow these steps:

1. Start configuring the configuration item by selecting Compliance Settings ➢ Company Resource Access.
2. Click VPN Profiles and choose Create VPN Profile in the Home tab of the ribbon. Supply a name and click Next. You can also import an existing VPN profile from a file, but in this example we will create a new PPTP profile.
3. As you can see in Figure 16.70, all major VPN brands are supported; the options on the Connection page will differ per brand. In this case choose PPTP, and therefore you need to supply a server list (with the VPN server friendly names and IP addresses), decide whether all network traffic must be sent through the VPN connection, and supply the connection-specific DNS suffix.

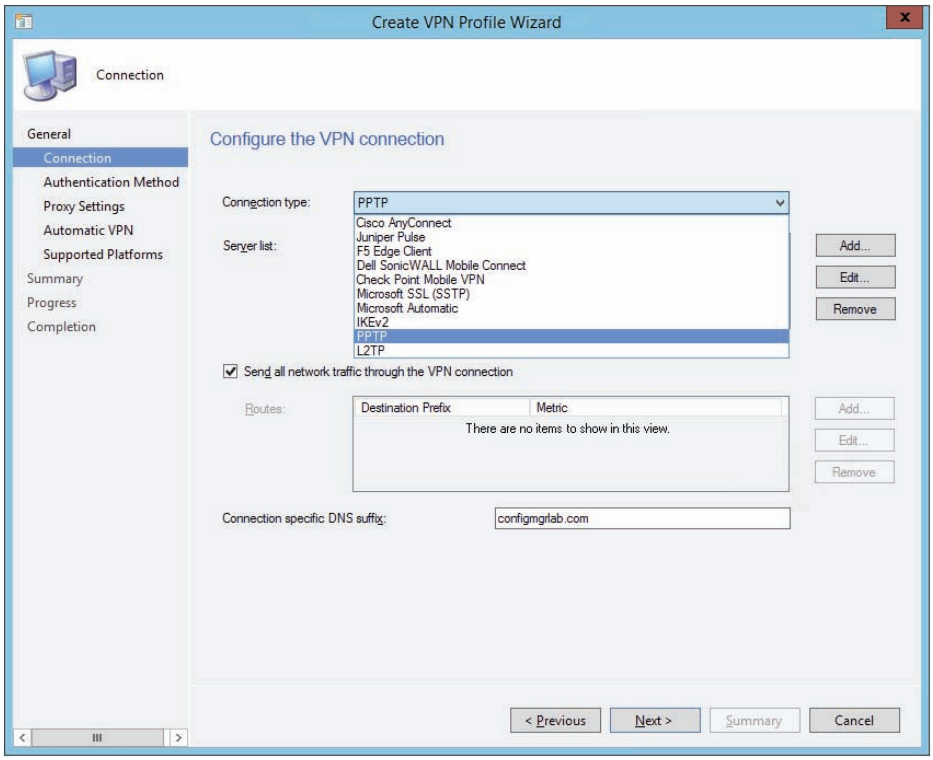


FIGURE 16.70
Create VPN Profile Wizard—Connection page

4. After configuring the Connection settings, click Next.
5. On the Authentication Method page, select the authentication method that is supported by the VPN device and click Next.
6. If necessary, configure proxy settings for the VPN profile. Define whether the proxy is automatically set or detected, or configure a proxy server to use. Click Next.
7. Enable VPN on-demand if you want the VPN connection to be started when a Native Windows 8.1 application is started. Supply the DNS suffix, the VPN server that uses that suffix, and when the VPN connection must be initiated, as shown in Figure 16.71.

   You can enable the Automatic VPN option while creating the Windows 8 application or on the General page of the Windows 8 Deployment Type.
8. Click Next to configure the supported Windows 8.1 and iOS platforms, and click Next again to move to the Summary screen.
9. Review the Summary page and click Next. Click Close when the VPN profile is created successfully.

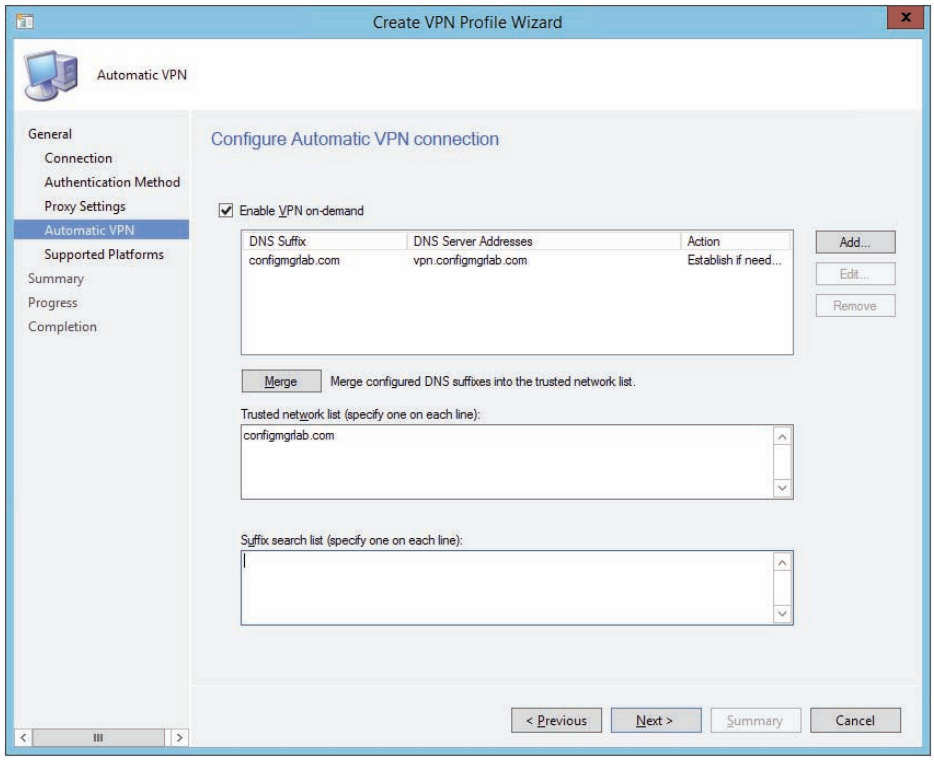


FIGURE 16.71 Create VPN Profile Wizard—Automatic VPN page

You can deploy the VPN profile to your test collections before rolling out the profiles to a broader range of mobile devices.

Finally, you can create Wi-Fi profiles to deploy to your corporate mobile devices. To create a Wi-Fi profile, follow these steps:

1. Start configuring the configuration item by selecting Compliance Settings ➢ Company Resource Access.
2. Click Wi-Fi Profiles and choose Create Wi-Fi Profile in the Home tab of the ribbon. Supply a name and click Next. You can also import an existing Wi-Fi profile from a file, but in this example we will create a new Wi-Fi profile.
3. The first step is supplying the general information about the Wi-Fi profile. Supply a network name and the SSID of the Wi-Fi network. You can also enable or disable the following options, as shown in Figure 16.72.
   - Connect Automatically When This Network Is In Range
   - Look For Other Wireless Networks While Connected To This Network
   - Connect When The Network Is Not Broadcasting Its Name (SSID)

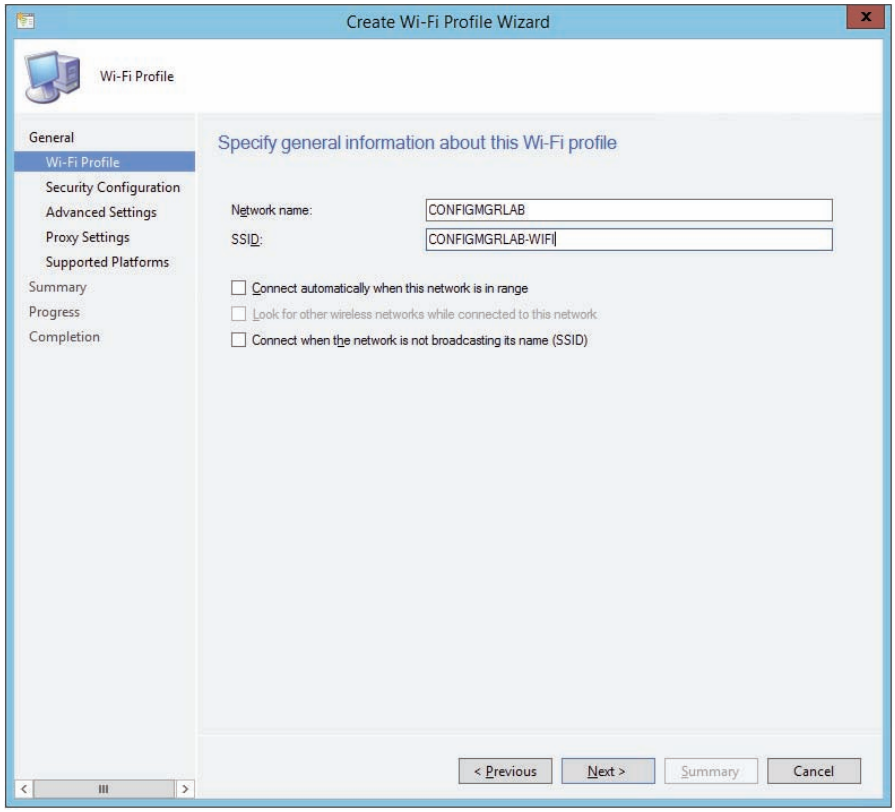


FIGURE 16.72
Create Wi-Fi Profile Wizard—Wi-Fi Profile page

4. The next step is to configure the security configuration. You need to configure a security type with the proper encryption information for your Wi-Fi network, as shown in Figure 16.73. Contact your network administrator for the appropriate information for your Wi-Fi network. Click Next to configure advanced settings. The advanced settings are not available for every security type.
5. If necessary, configure proxy settings for the Wi-Fi profile. Define whether the proxy is automatically set or detected, or configure a proxy server to use.
6. Click Next to configure the supported platforms. Click Next.
7. Review the Summary page and click Next. Click Close when the Wi-Fi profile is created successfully. Again, deploy the Wi-Fi profile first to your test collections before rolling it out in your environment.

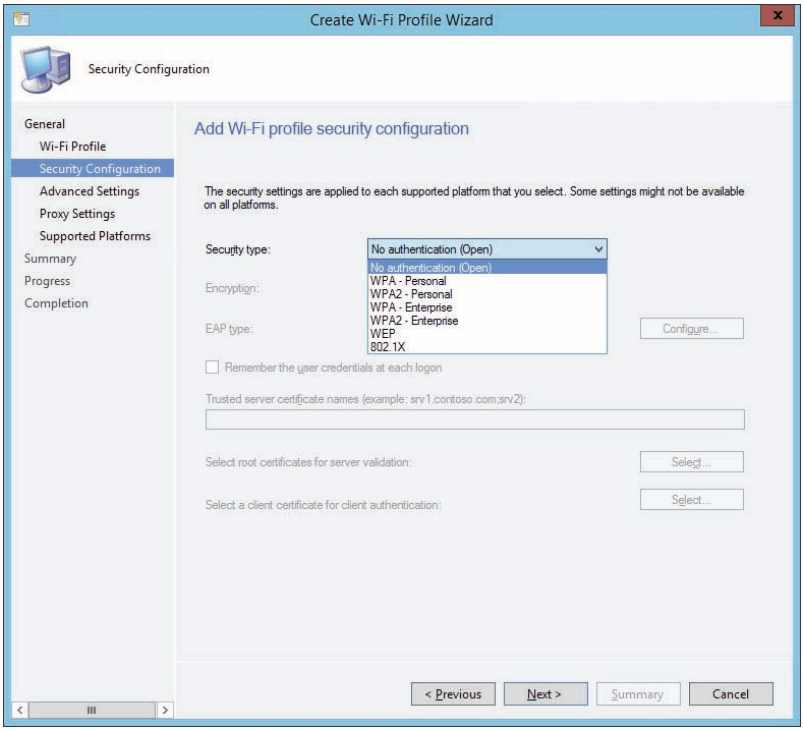


Figure 16.73
Create Wi-Fi Profile Wizard—Security Configuration page

Wipe vs. Selective Wipe

Letting mobile devices connect to your environment creates a risk when someone loses the mobile device or an employee leaves the company. Therefore several options are built into Configuration Manager 2012 R2 to make sure that the corporate data is removed when necessary. Before exploring the Wipe functionality, it is important that we explain a feature called Device Ownership.

Personal vs. Company-Owned Devices

In Configuration Manager you can configure a mobile device as personal or company owned. Every mobile device that is not joined to a domain and enrolled in Configuration Manager is configured as a personal device. You can change the ownership of a device as follows:

1. Start configuring the item by selecting Assets And Compliance ➢ Overview ➢ Devices in the Configuration Manager console.
2. Select the mobile device for which you want to change the ownership, and click Change Ownership in the Home tab of the ribbon.
3. Change the ownership from Personal to Company, as shown in Figure 16.74.
4. After changing the ownership, click OK.

By using the device ownership options you can create collections based on the global conditions and deploy software to your company-owned devices.

FIGURE 16.74
Edit Device Ownership dialog



WIPING A MOBILE DEVICE

You can wipe a mobile device via the Configuration Manager 2012 R2 console. Depending on whether the mobile device is personal or company owned and on the operating system, the procedure for wiping the device is different. Wiping a device can be done selectively or fully. Wiping a device fully basically initiates a factory reset of the mobile device the next time it connects to Configuration Manager.

The selective wipe experience will be a bit different on every supported platform, since not all platforms support the same features. Selective wipe can remove or revoke the following corporate information:

1. Email
2. Applications installed through the MDM channel (Windows Intune)
3. Wi-Fi profiles
4. VPN profiles
5. Certificates
6. MDM policies (settings)
7. Management agent
8. Corporate application data

Table 16.1 lists the features corresponding to the previous numbers per platform.

TABLE 16.1: Wipe features per platform

PLATFORM	FULL WIPE	1	2	3	4	5	6	7	8
Windows 8.1 (x86/RT OMA-DM managed)		✓	✓	✓	✓	✓	✓		✓
Windows 8 RT		✓		✓	✓	NA	✓	✓	
Windows Phone	✓		✓	✓	✓	✓	✓	✓	✓
iOS	✓		✓	✓	✓	✓	✓	✓	✓
Android						✓	✓	✓	

The features and the experience may differ per platform and version of Windows Intune. Consult the TechNet documentation for the latest status: `http://technet.microsoft.com/en-us/library/jj884158.aspx`.

Once you know what will be wiped, you can choose the right method if you need to selectively wipe a mobile device. Follow these steps:

1. Start configuring the item by selecting Assets And Compliance ➢ Overview ➢ Devices in the Configuration Manager console.
2. Select the mobile device you want to wipe, and choose Retire/Wipe in the Home tab of the ribbon.
3. Select either Wipe Company Content And Retire The Mobile Device From Configuration Manager (selective wipe) or Wipe The Mobile Device And Retire It From Configuration Manager, as shown in Figure 16.75. Click OK.

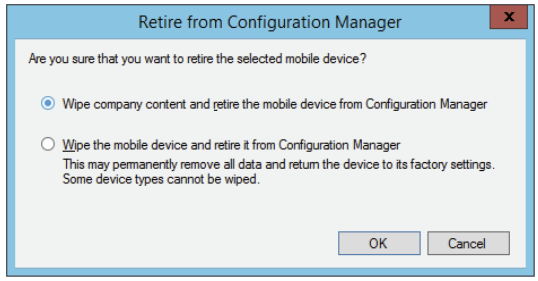


FIGURE 16.75
Retire From Configuration Manager dialog

Troubleshooting

The method of troubleshooting problems with mobile devices depends on the management mode chosen. For lite management, troubleshooting will be mostly focused on Exchange Server—both in terms of ensuring that the Exchange ActiveSync connector is running properly and ensuring that the Configuration Manager 2012 Exchange ActiveSync connector is properly configured and operational.

When it comes to depth management, there are a few more places to check when you run into problems. Depth-managed devices require enrollment before management can begin. The enrollment process is not difficult, but there are a number of moving parts that must be configured properly, not the least of which is certificates. When enrollment fails, it's clear on the device that there was a problem, but it's not always easy to collect diagnostic information from the device to understand why enrollment failed. Fortunately, there is excellent logging around the enrollment process to help. The `EnrollmentService.log` and `EnrollmentWeb.log` may contain errors that might occur as the enrollment process progresses. These logs are located in the `SMS_CCM` folder, under the `EnrollmentPoint\logs` and `EnrollmentProxyPoint\logs` folders, respectively.

When using the Windows Intune connector you have some different log files in the `%SMS_LOG_PATH%` folder. The log file `cloudusersync.log` will help you identify issues with synchronizing the users in the collection that holds the users who are allowed to enroll

their mobile devices. The log files `dmpdownloader.log`, `dmpuploader.log`, `dismgr.log`, and `outboundcontentmanager.log` will help you identify issues with uploading and downloading apps, policies, and messages from and to Windows Intune. If you have issues when installing the Windows Intune connector, look in the following log files: `sitecomp.log`, `connectorsetup.log`, and `certmgr.log`.

The depth-managed mobile device client has similarities to the computer device client in that client health data is provided. Simply reviewing a device in the collections to ensure client health evaluations are current and successful, along with checking the Client Status data from the Monitoring node, is a good indicator of whether the client is behaving properly.

The Bottom Line

Detail the differences between lite and depth management. The management options and settings available for mobile devices will vary depending on whether lite- or depth-management options are in place.

> **Master It** List mobile device management capabilities for lite versus depth management.

Understand how to configure mobile device management. Properly configuring mobile device management requires addressing several potential scenarios. From a Configuration Manager 2012 perspective, though, the choice is simple: lite or depth management.

> **Master It** List the items that need to be configured for both lite and depth management.

Understand the depth-management enrollment process. From the user perspective, the enrollment process for depth management is straightforward. Behind the scenes, there are a number of moving parts. Each of these components is critical to the enrollment process.

> **Master It** List the components required to enroll depth-managed devices.



Chapter 17

Role-Based Administration

Ask a System Center Configuration Manager administrator about one of the more challenging aspects of administering ConfigMgr in their environment, and they might answer "Security!" The class and instance model that was used in SMS and ConfigMgr 2007 to assign users varying levels of access and privileges was somewhat cumbersome and confusing.

System Center Operations Manager 2007 introduced the concept of role-based security administration to the System Center suite. Under the Role-Based Access Control (RBAC) model, administrators are able to use security roles and security scopes to define access to resources for the administrative users in the environment. System Center 2012 Configuration Manager adopts the RBAC security model and, as a result, greatly simplifies the administration of security in ConfigMgr 2012.

In this chapter, you will learn to

- Understand the role-based administration model in ConfigMgr 2012
- Distinguish security roles from security scopes
- Understand which objects in ConfigMgr 2012 define an administrative user
- Understand how to simulate permissions in the ConfigMgr 2012 console

Overview of Role-Based Administration

Configuration Manager 2012 uses the Role-Based Access Control model to define access to ConfigMgr features and functions. Under the RBAC model, the ConfigMgr 2012 administrator uses security roles, security scopes, and collections to define the administrative scope for the ConfigMgr administrative users. This provides the ConfigMgr administrator with the ability to define the security configuration for an administrative user in such a way that the only features of ConfigMgr 2012 that the user is able to view and interact with in the console are those that are part of their responsibility. All other items are essentially hidden and not available to the administrative user. This behavior is sometimes referred to as "Show me" behavior.

For example, consider a help desk analyst who needs the ability to deploy an application to computers in one geographic location but should not have the ability to deploy applications to computers in any other locations. Using the role-based administration model, the ConfigMgr administrator could easily create security roles, security scopes, and collections to satisfy those requirements. We will look at a sample scenario later.

One important new feature in Configuration Manager 2012 R2 is that reports can now utilize the role-based administration model. The data that is returned by all of the Configuration Manager reports will be filtered based on the permissions of the administrative user who is running the report. This greatly simplifies the process of securing access to report data.

Using Security Roles and Security Scopes

Security roles are used to organize tasks or functions, while security scopes are used to define access to objects. ConfigMgr 2012 provides some default roles and scopes, and the ConfigMgr administrator can also create their own to meet specific business needs. By using combinations of security roles, security scopes, and collections, the ConfigMgr administrator can easily control access to the environment and define what the ConfigMgr administrative users can view and manage.

As stated previously, this is sometimes referred to as "Show me" behavior and basically means that the administrative user will see only what is relevant to them and what they have access to in the ConfigMgr 2012 console. This is also known as access-based enumeration. Console objects that the administrative user has access to are visible in the console, while all others are hidden. This greatly simplifies the console experience for the administrative user and helps reduce confusion.

Managing with Flat Hierarchies

One of the design goals for ConfigMgr 2012 is that organizations should have flat ConfigMgr 2012 hierarchies. In fact, many companies may find they need only a single ConfigMgr primary site. One common reason for multiple SMS or ConfigMgr sites in previous versions of the product was to completely segregate the environment based on roles or functions. For example, one ConfigMgr 2007 primary site may have been used to manage only desktops and laptops, while another ConfigMgr 2007 primary site may have been used to manage only servers. Separating the sites completely ensured that the administrators for the desktop and laptop site could not manage the servers in any way and vice versa.

With the ability to designate control based on security roles, security scopes, and collections in ConfigMgr 2012, segregating the environment through the use of multiple primary sites is unnecessary. In ConfigMgr 2012, the ConfigMgr administrator could have all devices report to a single primary site and then use role-based security to define the required access for the administrative users. The desktop support team could be configured to see and manage only desktop computers, and the server team could be configured to see and manage only servers. Another benefit of the new security model in ConfigMgr 2012 is that the administrative objects (security roles, security scopes, and collections) need to be created only once in a ConfigMgr 2012 hierarchy with a Central Administration Site and child primary sites because that information is sent throughout the hierarchy as globally replicated data.

Security Roles

ConfigMgr 2012 uses security roles to define access to resources for administrative users. Security roles can be configured to provide administrative users with as much or as little access as they need in ConfigMgr to perform their job.

ConfigMgr 2012 includes several built-in security roles that handle many common ConfigMgr administrative task scenarios. Figure 17.1 shows the security roles that are included in ConfigMgr 2012. The following list provides a brief description of the built-in roles:

Application Administrator This role provides the permissions to perform both the application Deployment Manager role and the Application Author role. This role also provides the

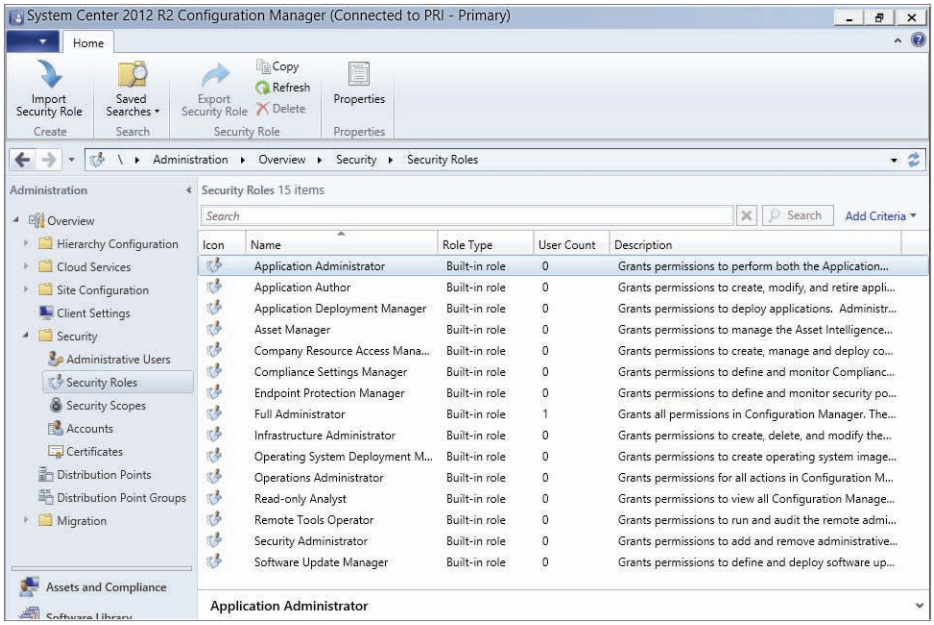


FIGURE 17.1 Built-in security roles

ability to manage queries, view site settings, manage collections, and edit settings for user device affinity.

Application Author This role provides the ability to create, modify, and delete applications. This role also provides the ability to manage packages and programs, manage alerts, and view status messages.

Application Deployment Manager This role provides the ability to distribute applications. Application deployment managers can view the list of applications and can manage other items related to applications, including alerts, templates, packages, and programs. They can view collections and collection membership and can also view status messages, queries, and conditional delivery rules.

Asset Manager This role provides the ability to manage the Asset Intelligence synchronization point, the Asset Intelligence reporting classes, hardware and software inventory, and software metering settings.

Compliance Resource Access Manager This role provides permissions to create, manage, and deploy the company resource access profiles. These include Wi-Fi, VPN, and certificate profiles to users and devices.

Compliance Settings Manager This role provides permissions to manage the Compliance Settings feature. Compliance Settings managers can create, modify, and delete configuration items and baselines. They can also deploy configuration baselines to collections, initiate compliance evaluation, and initiate remediation for noncompliant computers.

Endpoint Protection Manager This role provides the ability to manage and monitor Endpoint Protection security policies. Administrative users with this role can create, modify, and delete Endpoint Protection policies. They can also deploy Endpoint Protection policies to collections, create and modify alerts, and monitor Endpoint Protection status.

Full Administrator This role provides access to all objects. The administrator who installs ConfigMgr 2012 is automatically granted this security role.

Infrastructure Administrator This role allows the administrative user to create, delete, and modify the Configuration Manager Server infrastructure and also provides access to the site migration tasks.

Operating System Deployment Manager This role provides the ability to create operating system images and to deploy them to computers. Administrative users with this role can manage many aspects of the operating system deployment process, including the operating system installation packages and images, task sequences, drivers, boot images, and state migration settings.

Operations Administrator This role provides permissions for all actions in ConfigMgr 2012 except for the ability to manage security (managing administrative users, security roles, collections, and security scopes).

Read-only Analyst This role provides the ability to read all objects in ConfigMgr 2012.

Remote Tools Operator This role grants permissions to run and audit the remote administration tools. Administrative users with this role can use the ConfigMgr console to run the out-of-band management console and can use remote control, Windows Remote Assistance, and Remote Desktop Services.

Security Administrator This role provides the ability to add and remove administrative users and to associate administrative users with security roles, collections, and security scopes.

Software Update Manager This role provides the ability to define and deploy software updates. Administrative users with this role can create collections, software update groups, deployments, and templates and can enable software updates for Network Access Protection.

Full Administrator? Oh My!

As shown in the list, the Full Administrator role in ConfigMgr 2012 provides access to all objects in the environment. Users (or groups) who are assigned to this security role hold all the keys to all of the castles in the ConfigMgr 2012 environment. As a result, the number of users or groups who have this security role should be *very* limited. Because of the power that this role holds, the fewer the administrative users who have this role the better! Also, the organization should periodically review the access requirements for administrative users who hold this role and determine if they can be provided with a less-powerful security role.

As you can see in the preceding list, each security role provides specific permissions for various object types. If you want to see the permissions that a specific security role holds, you can view that information in the ConfigMgr 2012 console. For example, if you wanted

to examine the permissions for the Application Administrator role, you would perform the following steps:

1. In the Configuration Manager administrative console, select Administration ➢ Overview ➢ Security ➢ Security Roles.
2. Select the role that you want to inspect. In this case it is the Application Administrator role.
3. Click Properties in the Home tab of the ribbon.

   This will open the Application Administrator Properties window.
4. Select the Permissions tab.
5. Now you can view the permissions for the role (Figure 17.2).

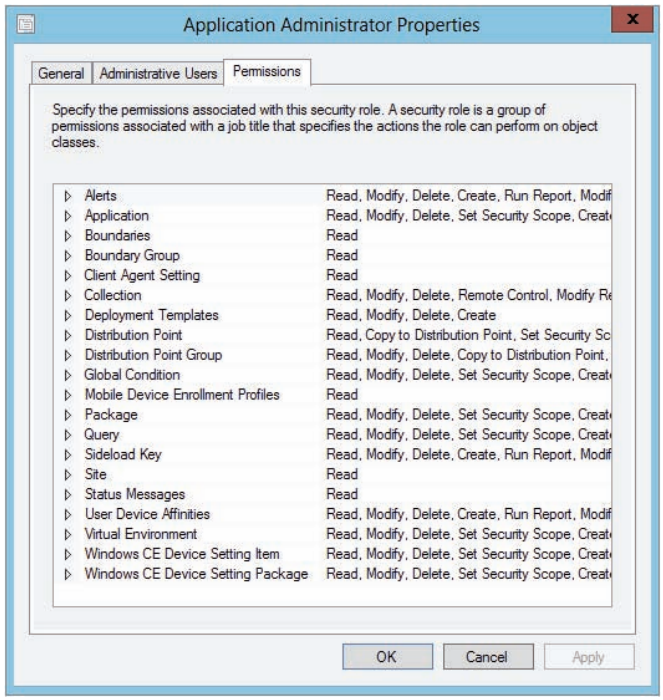


FIGURE 17.2 Application Administrator Properties

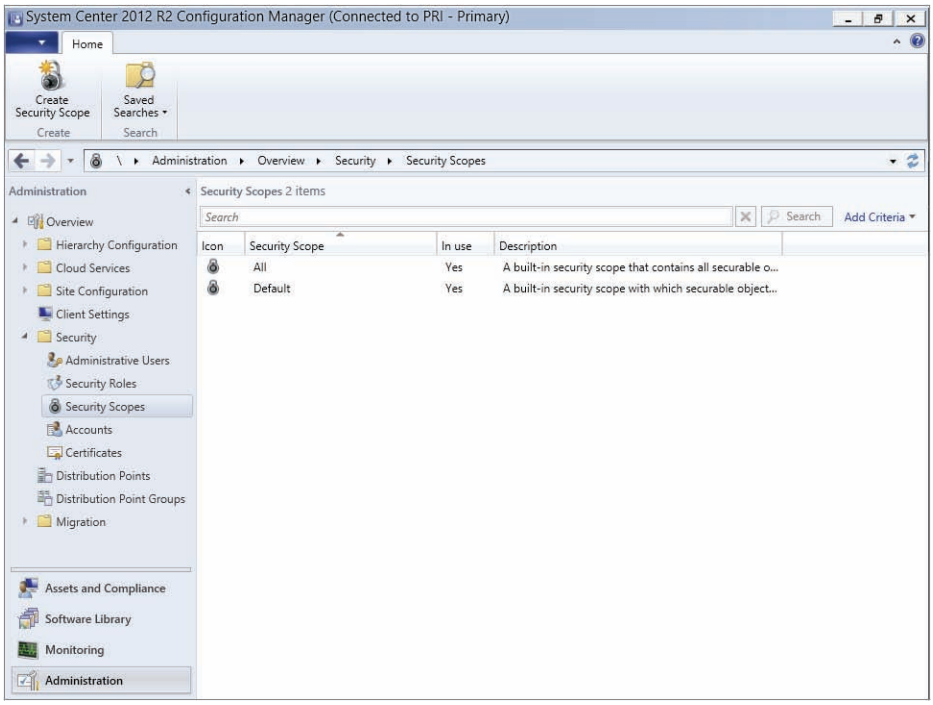
It is worth noting that you cannot change the permissions for the built-in security roles. You also cannot delete the built-in roles or export them. If you need to customize a built-in security role, then you should choose an existing role that is similar to the new role and make a copy of it. You will then have the ability to modify or delete the copied role. You can also export and import copied security roles. This import/export ability may be useful in a test or pilot ConfigMgr 2012 environment and would provide you with the ability to fine-tune the required security roles and permissions in the test site before deploying them to the production ConfigMgr 2012 site.

Also, if administrative users will perform multiple functions in ConfigMgr 2012 (such as deploy applications *and* use remote tools), the ConfigMgr administrator should assign multiple security roles to the administrative user instead of creating a new security role that combines a variety of tasks into a single role.

Security Scopes

ConfigMgr 2012 uses security scopes (Figure 17.3) to provide administrative users with access to secured objects. All secured objects must be assigned to at least one security scope. The association between the object and the security scope is managed from the object itself, not from the security scope.

FIGURE 17.3
Security scopes



As shown in Figure 17.3, ConfigMgr 2012 includes two built-in security scopes: All and Default.

All The All security scope grants access to all scopes. Objects cannot be assigned to this security scope.

Default All objects are assigned to the All security scope when ConfigMgr 2012 is installed. As new objects are added to ConfigMgr 2012, they are also automatically added to the Default scope.

The ConfigMgr administrator can also create custom security scopes that are based on the needs of the environment and add the objects to the custom scopes.

Creating a Custom Security Scope

The following are the steps to create a custom security scope:

1. In the Configuration Manager administrative console, select the Administration workspace ➢ Overview ➢ Security ➢ Security Scopes.
2. In the ribbon select Create Security Scope.
3. Provide a descriptive name for the security scope in the security scope Name field. In this case we will name our new scope Custom Security Scope.

   You can add a description and make changes to the administrative assignments if needed.
4. Once the changes have been completed, click OK.

The new security scope should now be visible in the console, as shown in Figure 17.4.

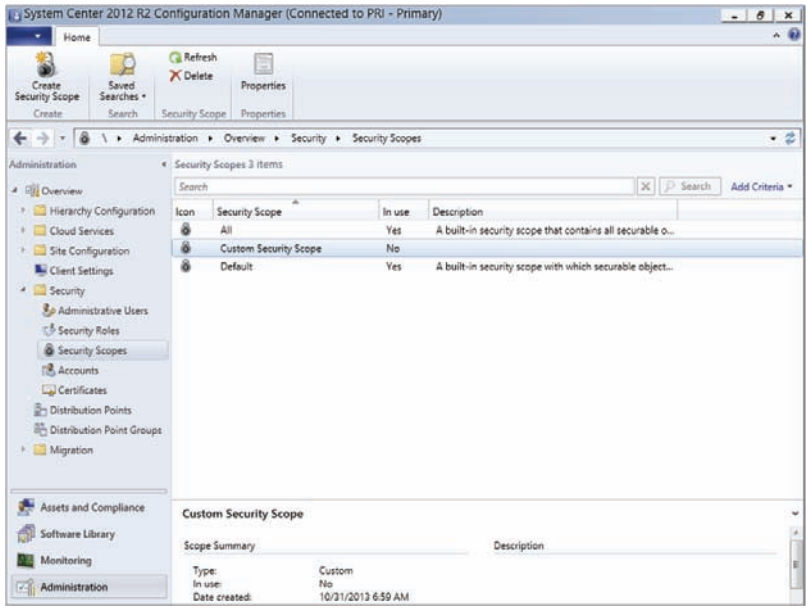


Figure 17.4
New security scope

Why Does the Column In Use Have a Value of No?

You may notice that the built-in security scopes (All and Default) show a value of Yes in the In Use column, while the security scope we just created has a value of No. The reason for this is we have not yet assigned objects to this new security scope. Once objects are assigned to the scope, it will automatically be changed to Yes. This allows the administrator to know which scopes have associated objects and which ones do not.

Security scopes can contain one or more object types, which include the following:

- Alert subscriptions
- Antimalware policies
- Applications
- Boot images
- Boundary groups
- Collections
- Configuration items
- Custom client settings
- Distribution points and distribution point groups
- Driver packages
- Global conditions
- Migration jobs
- Operating system images
- Operating system installation packages
- Packages
- Queries
- Sites
- Software metering rules
- Software update groups
- Software updates deployment packages
- Task sequences

Several object types cannot be included in security scopes and must be secured via security roles. These objects include the following:

- Active Directory forests
- Administrative users
- Alerts
- Boundaries
- Computer associations
- Default client settings

- Deployment templates
- Device drivers
- Exchange Server connectors
- Migration site-to-site mappings
- Mobile device enrollment profiles
- Security roles
- Security scopes
- Site addresses
- Site system servers and roles
- Software titles
- Software updates
- Status messages
- User device affinities

Assigning Resources to a Security Scope

Now that you understand how to create a security scope and you know which object types can be included, you will assign a resource to the new security scope you just created.

1. In the Configuration Manager administrative console, select the resource that will be added to the Custom Security Scope you created previously.

   Remember that only certain types of objects can be added to security scopes.

2. For this example we will select an application called XML Notepad, which was previously configured by another administrator.

3. Select Software Library ➢ Overview ➢ Application Management ➢ Applications in the ConfigMgr 2012 console, and choose the application that you want to manage.

4. Now choose the Classify section in the ribbon and then select Set Security Scopes.

   You could also right-click the application and select Set Security Scopes there.

5. In the Set Security Scopes window, select the desired scope or scopes for this object and click OK.

   For this scenario we will select only our new security scope, which we named Custom Security Scope in the previous exercise.

The new security scope should now be visible in the console (Figure 17.5).

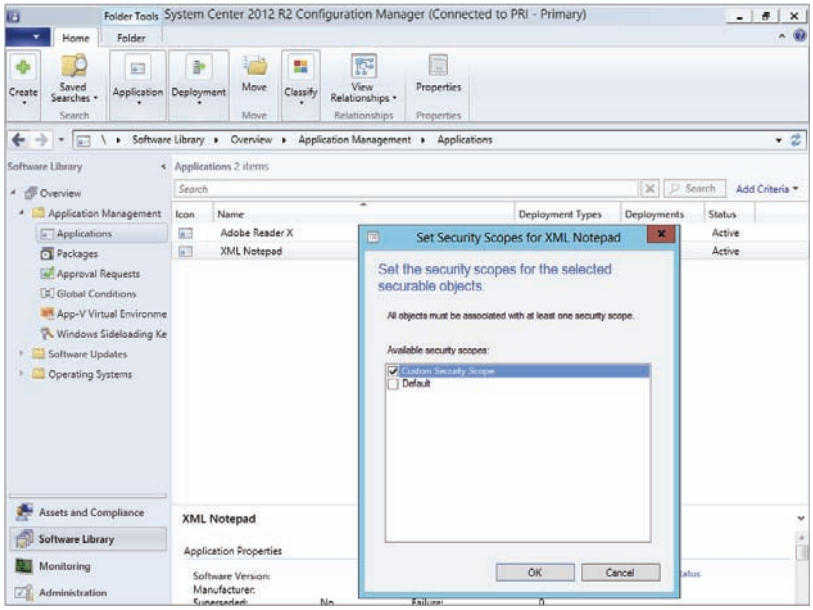


FIGURE 17.5
New security scope and application

6. Once the setting is applied, view the security scope and see that the In Use value is now set to Yes, as shown in Figure 17.6.

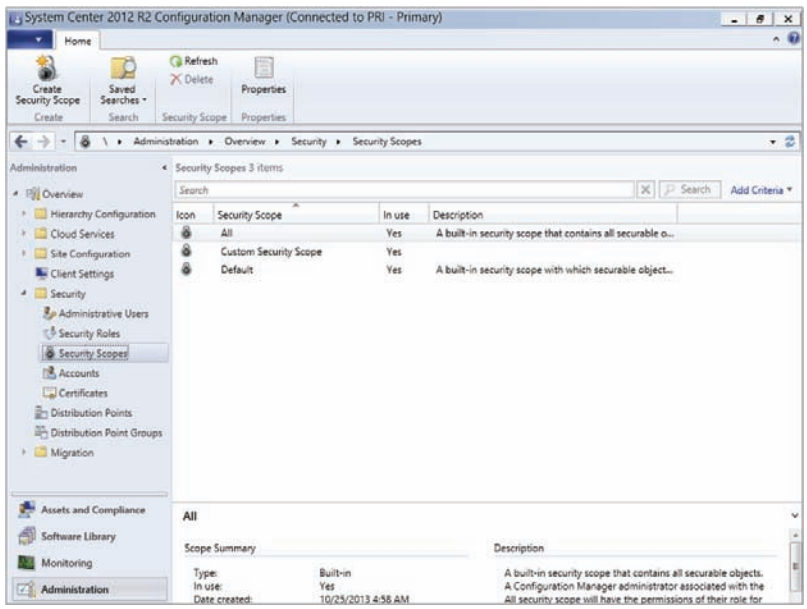


FIGURE 17.6
New security scope

Viewing Security Scope Objects

If you want to view all of the objects that are associated with a given security scope, a built-in report in ConfigMgr 2012 will provide that information.

1. In the Configuration Manager administrative console choose Monitoring ➢ Overview ➢ Reporting ➢ Reports.

   There are a few reports related to security scopes. The report we will run is titled Objects Secured By A Single Security Scope.

2. Right-click the report and select Run.

   For this example we will use Application <all values> for the Object Type field, and in the Security Scope field we will specify the scope we created previously. You can either enter the scope name in the field or select the Values option to list all known values for that particular field.

3. For this scenario we will use Custom Security Scope because this was the name we gave the security scope when it was created.

4. Once the values have been set, click View Report (Figure 17.7).

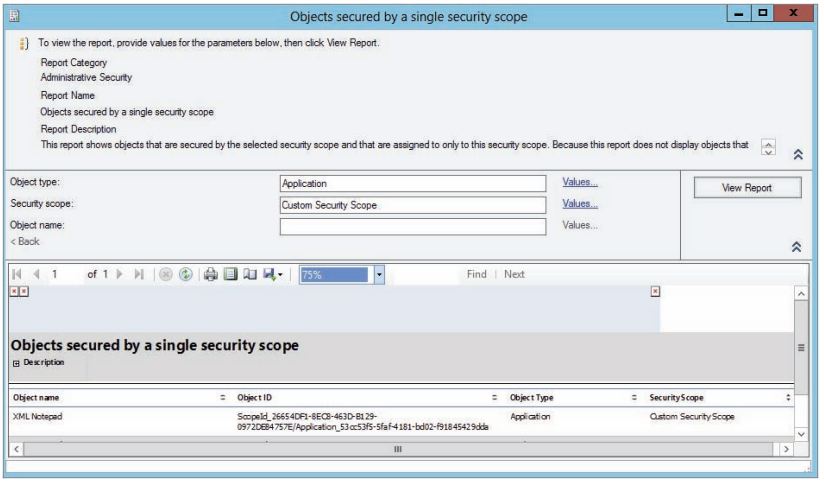


FIGURE 17.7
Objects Secured By A Single Security Scope report

This report is designed to show objects that are secured by only the specified security scope, which is Custom Security Scope in this scenario. If an object is secured by two or more security scopes (the Custom Security Scope and the default security scope, for example), then the object will not be displayed in this report.

Collections

We have discussed how security roles and security scopes are used in the role-based administration model in ConfigMgr 2012. In order for an administrative user to perform functions (for example, deploy an application) on a resource, the user must have access to a collection that contains the resource. We can use collections, along with security roles and security scopes, to tightly control what objects in the ConfigMgr console an administrative user can access.

Collections are probably not a new concept to the SMS and ConfigMgr veterans reading this book, but there are some changes to how collections work in ConfigMgr 2012. This chapter does not perform an exhaustive examination of those changes, but it does highlight some of the changes and differences.

Using Collections

As a bit of background, collections are a way to logically group resources, such as devices or users, and collections can be created to meet various manageability and targeting requirements. The following are just a few examples:

- Use collections to separate servers from workstations or laptops.
- Use collections to separate pilot users or devices from production resources.
- Use collections based on departments, business units, or geographical location for targeting or administrative purposes.

Once the requirements for the collection have been defined and the collection has been created, the collection can be assigned to a ConfigMgr administrative user.

Collections in ConfigMgr 2012 contain one or more rules that control the membership of the collection. There are four rule types:

Direct Rule This rule type allows the administrator to explicitly define the users or computers that should be members of the collection. The membership of this collection does not change unless the administrator removes the explicit entry in the collection properties or the resource is removed from ConfigMgr. You might think of this approach as hard-coding machine names into the collection membership properties.

Query Rule This rule type dynamically updates the membership of the collection based on a query that is run on a schedule by ConfigMgr. ConfigMgr uses query-based collections for the built-in collections. Query-based collections are very useful because they routinely evaluate the specified criteria and identify matching devices or users.

Include Collections Rule This new rule type allows the administrator to include members of another collection in a ConfigMgr collection. The membership of the current collection will be updated on a schedule when members of the included collection change.

Exclude Collections Rule This is another new rule type, and it allows the administrator to exclude the members of another collection from a ConfigMgr collection. The membership of the current collection will be updated on a schedule when members of the collection change.

Understanding the Default Collections

ConfigMgr 2012 includes a number of default collections. Some of these can be modified if need be, but none can be deleted. The following are the default collections:

All User Groups Contains user groups discovered during Active Directory Security Group Discovery.

All Users Contains users discovered during Active Directory User Discovery.

All Users And User Groups Contains the All Users and the All User Groups collections. This collection cannot be modified and contains the largest scope of user resources.

All Desktop And Server Clients Contains server and desktop devices that have the ConfigMgr 2012 client installed. Membership is determined by Heartbeat Discovery.

All Mobile Devices Contains mobile devices that are managed by ConfigMgr 2012. Membership is restricted to mobile devices that are successfully assigned to a site or discovered by the Exchange Server connector.

All Systems Contains the All Desktop And Server Clients, the All Mobile Devices, and All Unknown Computers collections. This collection cannot be modified and contains the largest scope of device resources.

All Unknown Computers Contains generic computer records for multiple computer platforms. It's typically used to deploy an operating system via PXE boot, bootable media, or prestaged media.

For more information about collections, see `http://technet.microsoft.com/en-us/library/gg682169.aspx`.

Administrative Users

An *administrative user* is an individual or group who will manage resources in the ConfigMgr 2012 infrastructure. The administrative user may have very limited access to resources in the environment (for example, a help desk analyst who can only deploy Adobe Reader X to computers in a specific office location) or may have complete access to all objects in the ConfigMgr environment (the ConfigMgr administrator).

The administrative user consists of a Windows user account (or a group) and at least one security role and one security scope. If needed, a collection could be used to limit the administrative scope of the administrative user (Figure 17.8). These items are configured when the administrative user is created and can be changed later if need be.

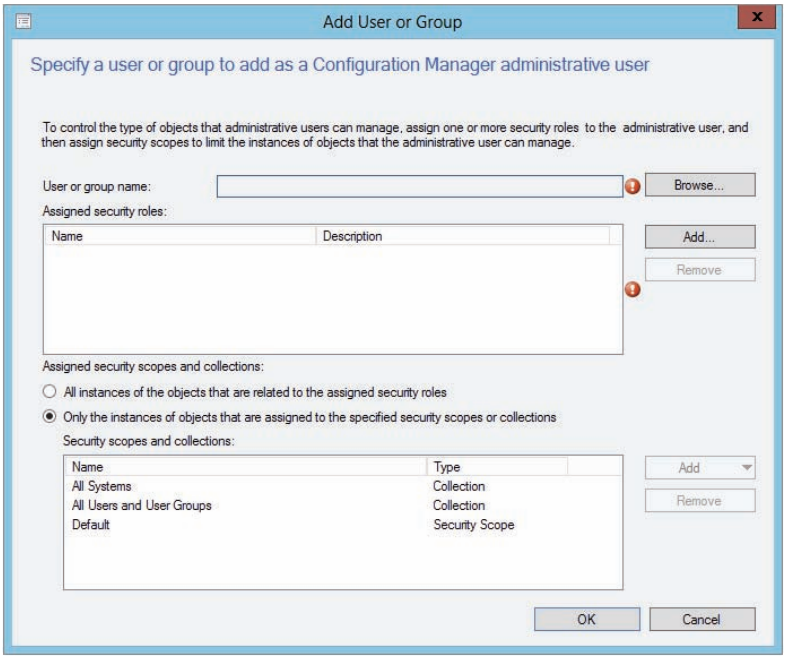


Figure 17.8
Assigned security scopes and collections

"Assigned Security Scopes And Collections"—What Does That Mean?

One issue that comes up during the administrative user creation process requires a bit more explanation. When you create a new administrative user, two options appear when you define the assigned security scope and collection for the user (see Figure 17.8).

The first choice is All Instances Of The Objects That Are Related To The Assigned Security Roles. If this option is selected, the administrative user will be associated with the All security scope and all collections.

The second choice is Only The Instances Of Objects That Are Assigned To The Specified Security Scopes Or Collections. This option allows the ConfigMgr administrator to add or remove security scopes and/or collections in order to provide a customized administrative scope for the user.

If you modify an administrative user, a third option is available called Associate Assigned Security Roles With Specific Security Scopes And Collections. As the wording of the option implies, this option allows the administrator to create associations between security roles, security scopes, and collections for the user.

We will now apply what you have learned and walk through a real-world scenario.

Real World Scenario

Helping the Help Desk Analyst

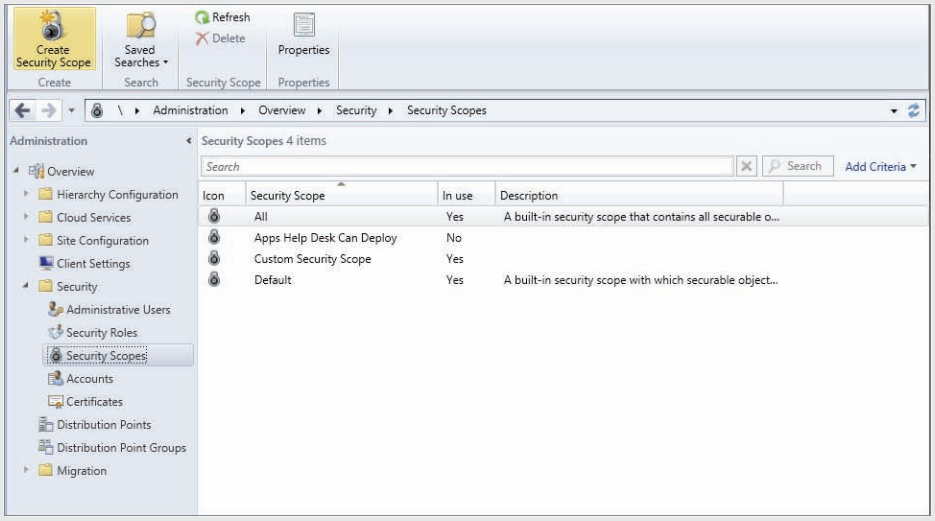
You are the ConfigMgr 2012 administrator and have been asked to provide ConfigMgr access to an administrative user. A help desk analyst needs the ability to deploy Adobe Reader X to all computers in the Dallas location. The analyst should also have the ability to use remote tools on the computers in the Dallas location. The analyst should not be able to deploy any other software to or interact in any way with the other computers in the infrastructure.

Which Security Role(s) to Use

As the ConfigMgr administrator, you first need to identify whether any of the existing security roles meet the needs of the scenario. In the ConfigMgr 2012 console, select Administration ➢ Overview ➢ Security ➢ Security Roles to view the roles that have been defined. The built-in Application Deployment Manager role appears to meet the requirements for the application delivery portion of the requirements. The built-in Remote Tools Operator role appears to meet the requirements for the remote tools functionality. So, you appear to have two existing security roles that will meet your needs. Later in this chapter you will learn how to use the RBA Viewer application to create custom security roles if need be.

You Need a Security Scope

The next step is to define the required security scope for the help desk analyst. The requirements stated that this user should only be able to deploy Adobe Reader X, so you need to create a security scope. You will use the process defined earlier in this chapter to create the security scope, and you will call the security scope Apps Help Desk Can Deploy. (See the following illustration.)



Remember that the In Use column value will be No until the security scope is associated with at least one object.

You may remember that the association between an object and the security scope is managed from the object, not from the security scope. So, you need to associate the security scope you just created with the Adobe Reader X application by performing the following steps:

1. In the ConfigMgr 2012 console, select the Adobe Reader X application in the Software Library workspace (Software Library ➢ Overview ➢ Application Management ➢ Applications).

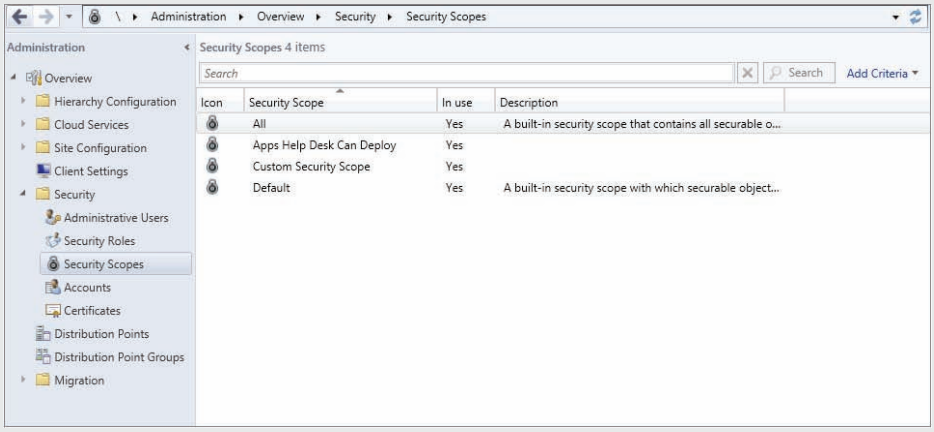
   For the purposes of this scenario, assume that an administrator has already created and configured the Adobe Reader X application installation in ConfigMgr 2012 and it is ready for deployment.

2. Right-click the Adobe Reader X application and select Set Security Scopes.
3. Uncheck the Default security scope, and check the Apps Help Desk Can Deploy security scope.
4. Click OK. (See the following illustration.)



Note: You may also need to include a distribution point or a distribution point group in the security scope in order for the Deploy Software Wizard to complete when executed under the administrative user's credentials.

If you go back and view the status of the Apps Help Desk Can Deploy security scope in the ConfigMgr console, it should now show a value of Yes in the In Use column.



And Now You Need a Collection

There are several ways to create the collection for this scenario. In fact, someone else may have already built a collection that includes the Dallas computer devices, and you could use that collection for your scenario.

However, let's assume you don't already have a collection that meets your needs and you need to create one. You may already know the names of the computers in the Dallas location and you could simply create a direct membership collection and directly add the computer names to the collection. Or, you could create a query-based collection and use data that is unique to the Dallas site to find computers that match the criteria. Examples of the data could be an Active Directory site, an Active Directory organization unit, certain TCP/IP subnet ranges, a certain naming standard in the computer names, and so on. For now, assume that you were provided a list of computers in Dallas, and you're going to add them to a direct-membership device collection called Dallas Computers.

Finally: Creating the Administrative User

You have gone through several steps to prepare the required access in ConfigMgr. This may seem rather labor intensive at first, but you created several items that may be used multiple times in future security configuration requests. Let's take a moment to review what you will be using to create the administrative user.

You are going to use two built-in security roles for this scenario: Application Deployment Manager (so the analyst can deploy Adobe Reader X to the Dallas computers) and Remote Tools Operator (so the analyst can use remote tools on the Dallas computers).

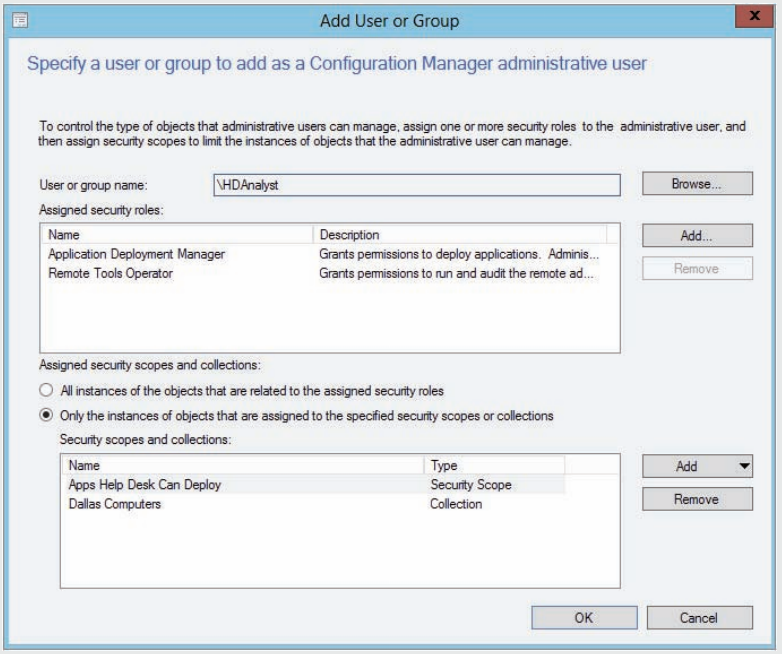
You created a security scope called Apps Help Desk Can Deploy and associated the scope with the Adobe Reader X application. This limits the help desk analyst to the Adobe Reader X application.

You created a direct-membership collection that contains the computers in the Dallas location.

The next step is to create the actual administrative user:

1. In the ConfigMgr 2012 console, select Administration ➢ Overview ➢ Security ➢ Administrative Users.
2. Either select the Add User Or Group option in the ribbon or right-click the Administrative Users option and select Add User Or Group.

   You need to designate the user or group that is being configured as an administrative user. In this scenario you are managing a single user.
3. Select the user's domain account (named HDAnalyst in this example). It is not part of the user name.
4. In the Assigned Security Roles section, use the Add option to select the security roles that you decided to use for this scenario: Application Deployment Manager and Remote Tools Operator.
5. In the Assigned Security Scopes And Collections section, select the Add option to choose the predefined collection and security scope that will limit what the help desk analyst has access to in the console. (See the following illustration.)



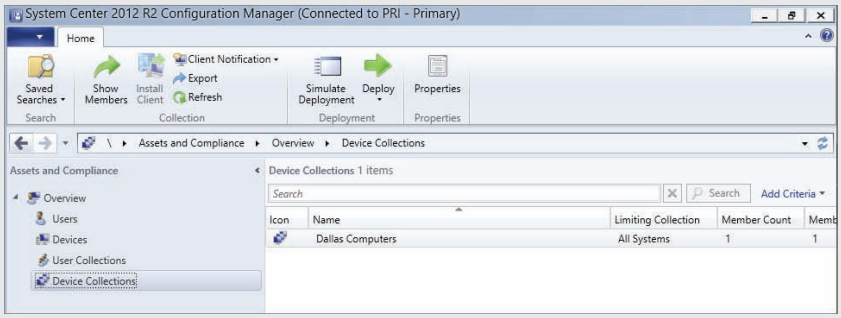
6. After adding the entries, click OK.

If there were several help desk analysts who needed the same configuration, you would probably create a group in Active Directory, add the users to that group, and then configure that group as an administrative user and avoid having to repeat these steps for each user individually.

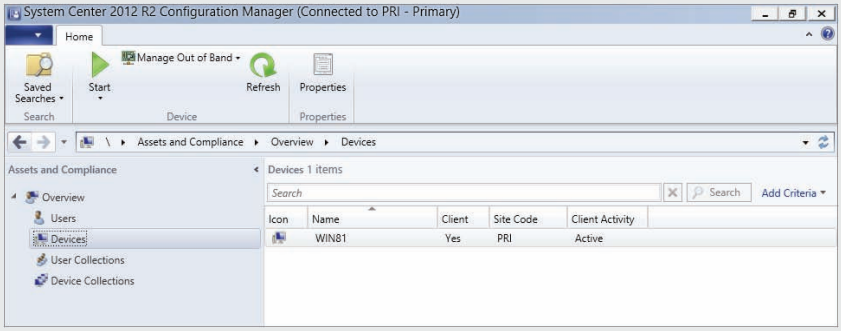
At this point you have completed your work and are ready for the help desk analyst to test their ConfigMgr 2012 console with their logon credentials and make sure they can perform the required functions.

If you performed the configuration properly, then the administrative user HDAnalyst should be able to open the ConfigMgr 2012 console and do the following:

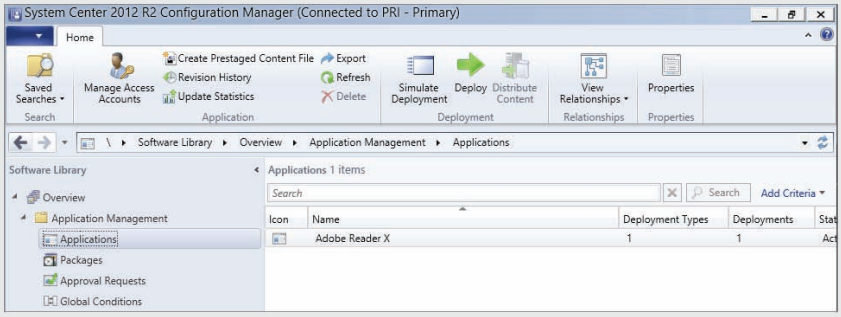
- View only the Dallas Computers collection in the Assets And Compliance ➢ Overview ➢ Device Collections view. (See the following illustration.)

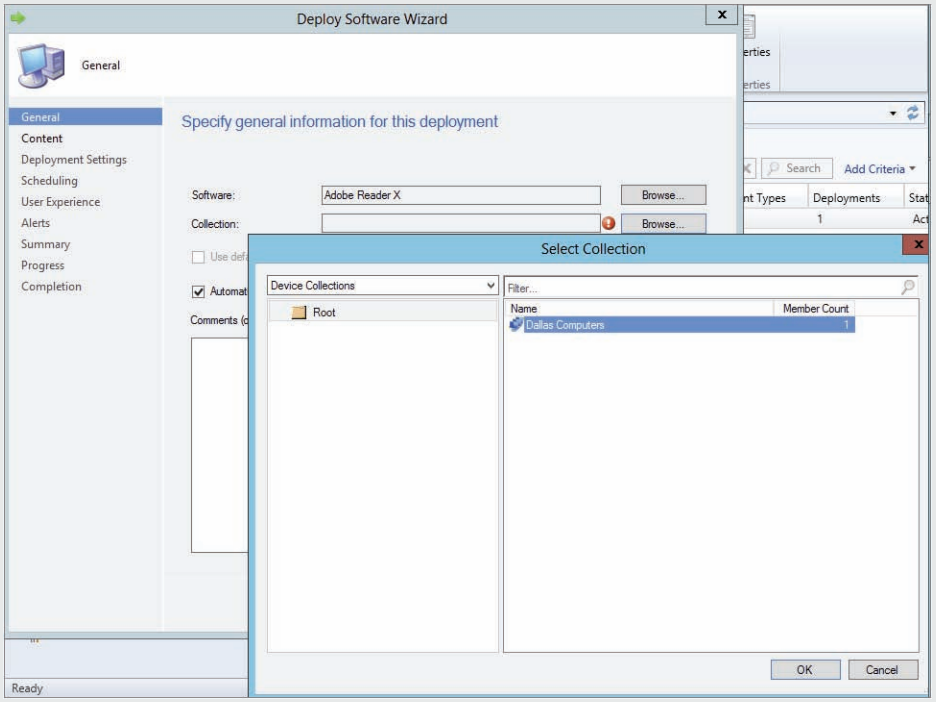


- See only the Dallas devices in the Assets And Compliance ➢ Overview ➢ Devices view. Also since the user can see only the Dallas devices, they can also use only remote tools against those computers. (See the following illustration.)

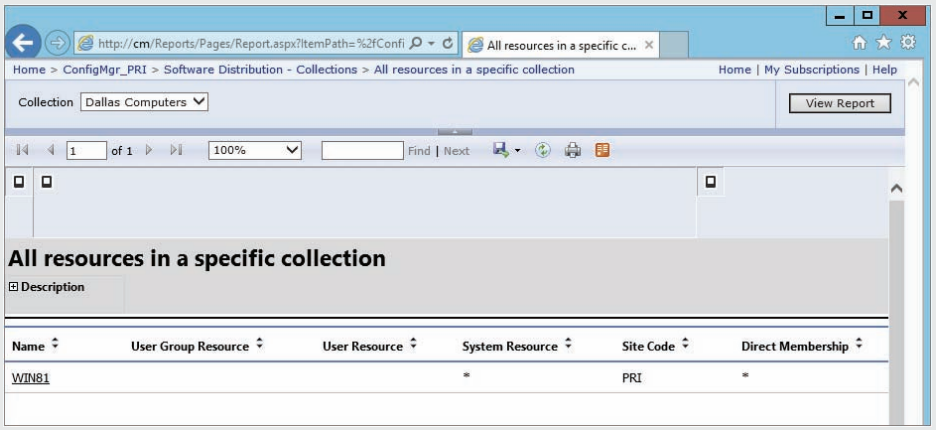


View only the Adobe Reader X application in Software Library ➢ Overview ➢ Application Manager ➢ Applications, and when they deploy it, they should only be able to select the Dallas Computers collection. (See the following illustrations.)





Also, as you learned earlier, Configuration Manager 2012 R2 uses the role-based administration model for reporting data as well. The HDAnalyst user should only be able to view report data about objects that the user has access to. If you open the reporting site and select the report titled All Resources In A Specific Collection, the user can only select the Dallas Computers collection and view data about the computers in the collection. (See the following illustration.)



RBA Viewer

You may already be familiar with the System Center 2012 Configuration Manager toolkit. It includes many useful utilities and tools that will help you manage your ConfigMgr environment and is available here:

```
www.microsoft.com/en-us/download/details.aspx?id=36213
```

One of the tools included in the toolkit is officially titled the Role-Based Administration Modeling and Auditing Tool, but the utility is commonly referred to as RBA Viewer. The RBA Viewer application allows you to model security roles with a specific set of permissions and also allows you to audit the security scopes and security roles of other ConfigMgr users. RBA Viewer should be very helpful as you develop the ConfigMgr security configuration for your environment.

The RBA Viewer application has a few requirements:

- The ConfigMgr 2012 console must be installed on the same computer as the RBA Viewer application.
- The user running the RBA Viewer application must be a member of the Full Administrator, Read-Only Analyst, or Security Administrator role.
- The user running RBA Viewer must be assigned to all security scopes and all collections.
- To analyze report folder security, the user must have SQL access and in order to analyze report drill through the RBA Viewer application must run on the site that has the Reporting Services point installed.

We will use a case study to demonstrate how to use RBA Viewer to create a new security role and verify that it will meet your needs.



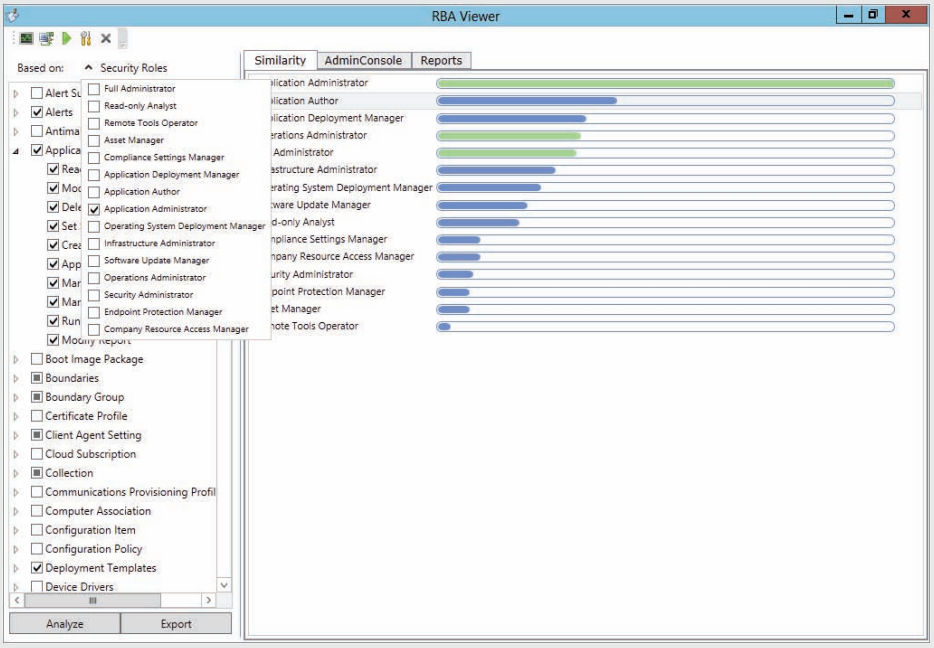
Real World Scenario

Creating an Administrative User

You are the ConfigMgr 2012 administrator and have been asked to provide ConfigMgr access to an administrative user. The user will need the access provided by the Application Administrator security role but also will need the added ability to create and modify software metering rules. You will use the RBA Viewer to define the new security role, verify that it meets the requirements, and then export it from RBA Viewer so that it can imported into the ConfigMgr console. Click Start ➢ ConfigMgr 2012 Toolkit and select RBA Viewer to open the RBA Viewer application.

1. In RBA Viewer you have the option to select a default security role and use that as a starting point for the required permissions, or you can start with an empty list of permissions. For this scenario we are adding additional permissions to the Application Administrator role so we will select the Application Administrator role from the list in RBA Viewer.

2. Verify that the Show Roles option is selected by clicking the icon in the top right of the RBA Viewer application and then select Application Administrator from the list of available security roles in the drop-down. See the following illustration.



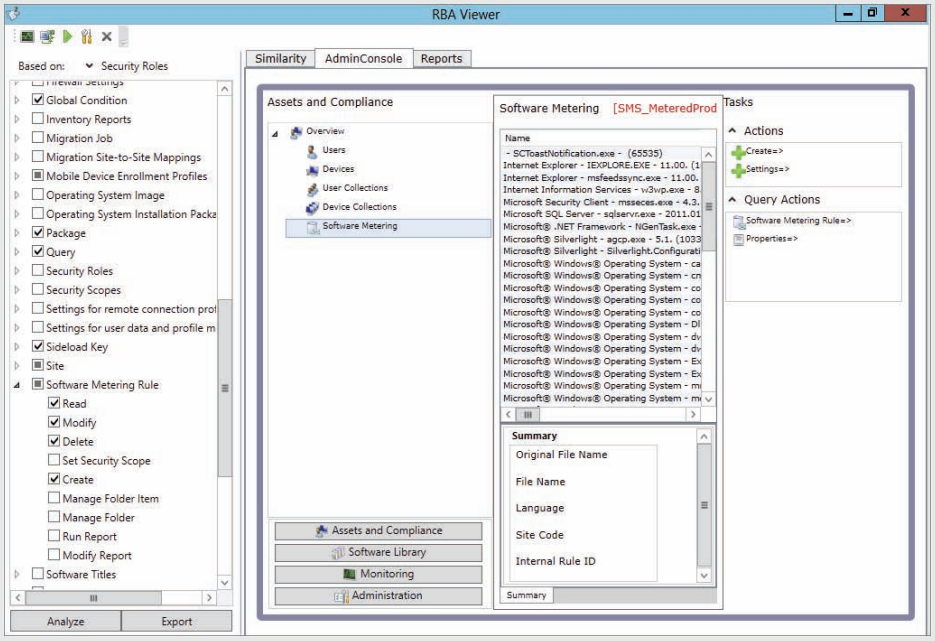
3. In this example we are adding the ability to create and modify software metering rules to the permissions provided by the Application Administrator role. Scroll down in list of available items and select Software Metering Rule Under Software Metering Rule, select Read, Modify, Delete, and Create.

4. Once the required permissions have been configured click Analyze. RBA Viewer will identify any existing security roles that are similar to the permissions that have been configured in the tool.

5. Select the AdminConsole tab in the RBA Viewer to verify that the user with this security role has the proper access. With this custom security role you should have the access provided by the Application Administrator role as well as the ability to manage software metering rules. You can also use the AdminConsole feature in RBA Viewer to verify that the security role cannot access or view other settings. See the following illustration.

6. Once the permissions have been properly configured, click the Export button. This will save the security role configuration to an XML file, which you can then import into the ConfigMgr 2012 console.

7. Open the ConfigMgr 2012 console and select the Administration workspace.



8. Select Overview ➢ Security ➢ Security Roles and choose the Import Security Role option from the ribbon.
9. At the Import Security Role window, select the XML file that you exported from RBA Viewer and click Open.
10. ConfigMgr 2012 will import the information from the XML file and create the security role. The security will use the name of the import file as the name of the new security role, but you can change the name if needed in the ConfigMgr console. You can also open the role and use the Permissions tab in the properties to ensure the correct permissions have been created for the role.

The Bottom Line

Understand the role-based administration model in ConfigMgr 2012. SMS and ConfigMgr 2007 used a class and instance security model, which could be confusing at times. ConfigMgr 2012 adopts the RBAC model, thereby making the administration of security in ConfigMgr 2012 a less-daunting task.

Master It What does RBAC stand for? And what does role-based administration mean?

Distinguish security roles from security scopes. Security roles and security scopes are important components of the role-based security model in ConfigMgr 2012.

Master It Can you identify the key differences between a security role and a security scope?

Understand which objects in ConfigMgr 2012 define an administrative user. The administrative user consists of the security role, the security scope, and collections. In this chapter you learned the differences between a security role and a security scope, and you know that collections can be used to control the objects that an administrative user can access.

> **Master It** As the ConfigMgr 2012 administrator, do you need to create a custom ConfigMgr 2012 console so that the administrative user can see only what you want them to see?

Understand how to simulate permissions in the ConfigMgr 2012 console. The RBAC model in ConfigMgr 2012 greatly simplifies the process for creating administrative users and defining what objects in ConfigMgr they can access.

> **Master It** Besides the ConfigMgr 2012 console itself, what other tool can you use to simulate ConfigMgr user security and verify that the security model will provide the desired level of access?



Chapter 18

Disaster Recovery

No matter what kind of hardware you are using for your Configuration Manager sites, there is always the possibility that hardware or some other failure will bring a site down. The only thing you can really do to prepare for something like this is to back up Configuration Manager the best you can so that you can get your site back up and running as soon as possible. Fortunately, Microsoft continues to include the Backup ConfigMgr Site Server maintenance task, which can be used to create a site backup that will provide the information you need to successfully recover your site server. In addition to the native application backup capabilities, Configuration Manager 2012 also supports two additional recovery methods. You can restore your Configuration Manager site from a site server database backup that is performed as part of a Microsoft SQL Server maintenance plan, or you can restore your site from a backup that is performed using System Center 2012 Data Protection Manager (DPM). The primary focus of this chapter will be on the configuration and usage of the Backup Site Server maintenance task.

In this chapter, you learn to

- Configure backups for Configuration Manager sites
- Recover Configuration Manager sites
- Archive backup snapshots to another location
- Reinstall the site components and reset file and registry permissions to their default settings

Planning for Disaster Recovery

Planning for disaster recovery in Configuration Manager is not complicated, but as you'll see in the section "Recovering Configuration Manager," it is different than it was in Configuration Manager 2007 and previous versions of System Management Server (SMS). With that in mind, you should consider the following when you are setting up your backup and recovery plans for your Configuration Manager hierarchy.

- The Configuration Manager backup task uses the Volume Shadow Copy Service (VSS), which is a part of the Windows Server operating system and is configured during the installation of Configuration Manager, to make backup snapshots.

Microsoft describes VSS as "a framework which facilitates communication between applications, storage subsystems, and storage management applications (including backup applications) in order to define point-in-time copies of storage data." The shadow copies that are made from VSS of the site server and the site database information are used to back up and restore Configuration Manager. By using VSS, the Backup ConfigMgr Site Server maintenance task can keep server downtime for backups to a minimum.

- A complete backup of a Configuration Manager site server includes the following:
  - The Configuration Manager site database (SQL)
  - The Configuration Manager site database transaction log
  - *<ConfigurationManager installation dir>*\Bin
  - *<ConfigurationManager installation dir>*\Inboxes
  - *<ConfigurationManager installation dir>*\Logs
  - *<ConfigurationManager installation dir>*\Data
  - *<ConfigurationManager installation dir>*\srvacct
  - *<ConfigurationManager installation dir>*\install.map
  - HKLM\Software\Microsoft\SMS registry keys on the site server
- Unlike most other SQL applications, the master SQL database isn't needed to restore a Configuration Manager site, so it isn't backed up with the Configuration Manager database when the Backup ConfigMgr Site Server maintenance task is run.
- If you have a site hierarchy with a Central Administration Site and multiple primary sites, a newly installed primary site will automatically receive all global data when the site is reinstalled.

What about Secondary Sites?

There is no backup task for Configuration Manager 2012 secondary sites, but there is a recovery option. If you need to recover a secondary site, you can select the site in the Configuration Manager console and initiate the recovery process. The secondary site will be reinstalled and the necessary data will be replicated from the primary site. This will be discussed in more detail later in the chapter.

What Is Not Included in the Backup

When planning for a backup, it is also very important to know what is *not* part of the backup maintenance task. As a rule of thumb, only the site server and the site database are included. You must also plan for the backup of remote site systems, add-on products, the content library, and the like.

The Content Library

The content library contains all packages (software updates, applications, and images). You will find a content library on the site server and all distribution points. You should consider adding these items to your enterprise backup solution. As a consequence of not backing up the content library, you may need to add several hours to the restore process because all files must be processed from the original source folders and inserted into the content library. With that in mind, also consider where you place source folders for any package. Organizations often host source files on the site server. This is not a recommended strategy; instead you should host all source folders on a separate file server.

Site Systems

The consequence of having a remote site system that fails is often a reinstallation of the specific site system. It is no big issue because most site systems cannot contain data and can be reinstalled quickly. Add to that the fact that you can have multiple instances of the same site system in the environment.

Configuration Manager Logs

The Backup ConfigMgr Site Server maintenance task will back up the log files located in the `Logs` folder (*`ConfigMgrInstallationPath`*`>\Logs`), but some Configuration Manager site system roles may write log files in other locations on the site server and these files are not backed up. If these log files should be backed up, you need to include them in your enterprise backup solution.

Clients

No client will be backed up during the backup maintenance task. In the event of a client failure, the new built-in client remediation task will be able to fix the error and perform a client reinstallation if needed.

SQL Reporting Services

Any customizations made to the default reports and custom reports will be lost in the event of a failure. All default reports will be recovered during the reinstallation of the site system.

When planning for a SQL Reporting Services backup you need to consider the following:

- Use the full recovery model in SQL to back up the reportserver database.
- Use the simple recovery model in SQL backup to back up the reportservertempdb database.
- Back up the encryption keys, using the rskeymgmt utility or the Reporting Services Configuration Manager.
- Back up these configuration files:
  - `Rsreportserver.config`
  - `Rssvrpolicy.config`
  - `Rsmgrpolicy.config`

- `Reportingservicesservice.exe.config`
- `Web.config` for both the Report Server and Report Manager ASP.NET applications
- `Machine.config` for ASP.NET

- Back up any custom reports, models, and custom projects.

For more detailed information about backing up SQL Reporting Services, see

`http://msdn.microsoft.com/en-us/library/ms155814.aspx`

WSUS Database

Windows Server Update Services is not part of the backup, and you should consider performing a regular backup using SQL, as described in this article:

`http://technet.microsoft.com/en-us/library/ms187510.aspx`

System Center Updates Publisher

System Center Updates Publisher (SCUP) is a stand-alone product installed with a single database stored in the user profile. You either need to perform a backup of the database from the user profile or configure SCUP 2011 to use a database from a shared network location.

To configure SCUP 2011 to use a database in `E:\SCUPDB`, follow these simple steps:

1. Open Windows Explorer and navigate to `C:\Users\Installation account\AppData\Local\Microsoft\System Center Updates Publisher 2011\5.00.1727.0000\`.
2. Copy the database file to a shared location.
3. Navigate to the SCUP 2011 installation folder and edit the `scup2011.exe.config` file.
4. Find `<setting name="SSCEDataFile" serializeAs="String">`.
5. Add this line: `<value>E:\SCUPDB\scupdb.sdf</value>`
6. Save and close the file.

With the database file on the network, all you need is a backup of the file.

Microsoft Deployment Toolkit

Microsoft Deployment Toolkit (MDT) is a free stand-alone tool from Microsoft that is often used with Configuration Manager 2012. MDT can contain a SQL database that you need to include in the normal SQL backup routines. Furthermore, you need to make sure that you have a backup of any custom scripts.

User State Migration Data

The files and folders that are used to store user state data on the Configuration Manager state migration point are not backed up as part of the Backup ConfigMgr Site Server maintenance task. You should determine if these folders and files should be backed up as part of your enterprise backup solution.

Backing Up Configuration Manager

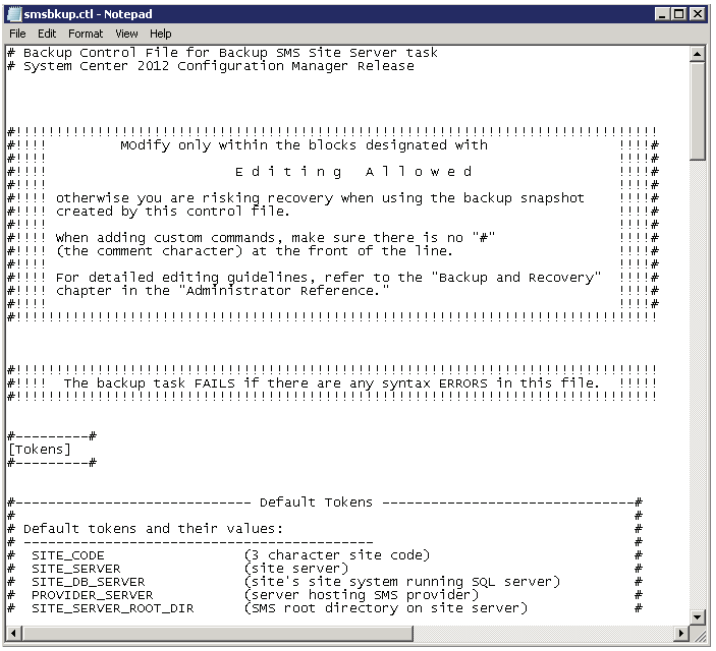
The first thing to know about backing up Configuration Manager sites is that you can automate the procedure by scheduling the Backup ConfigMgr Site Server maintenance task. We will cover this maintenance task in more detail later in the chapter.

When the Configuration Manager backup service (SMS_SITE_BACKUP) starts at the scheduled day and time, it uses instructions in the backup control file, located at

```
<ConfigMgr Install Location>\Inboxes\smsbkup.box\smsbkup.ctl
```

You can modify this file in Notepad to change what the backup service takes a snapshot of, but it isn't usually necessary. If you modify the file, take care not to change any of the default settings. Customizations that might be valuable to add are other registry keys or file locations. Figure 18.1 shows the default `smsbkup.ctl` file.

FIGURE 18.1
The `smsbkup.ctl` file


smsbkup.ctl - Notepad
File Edit Format View Help
Backup Control File for Backup SMS Site Server task
System Center 2012 Configuration Manager Release
#!!!

when you back up and restore the Central Administration Site that make it different than other primary sites when you set up backups of the central site and when you recover them:

- The Central Administration Site is the busiest site in your hierarchy, which gives you a smaller time frame for scheduling a backup. Configuration changes are made on a constant basis, and you may not be able to recover them all.
- The Central Administration Site has the largest amount of data, because it is the only site that contains all global and site data. It will take longer to back up than your primary sites.

These combined factors might make you consider backing it up less frequently than your primary sites. But this is not a good idea, because the Central Administration Site is the most important site in your Configuration Manager hierarchy. If one of your primary sites fails, and for some reason your backups for that site are corrupted, you can always install a new primary site and replicate the most current global data from the Central Administration Site. That's not the case with the Central Administration Site. With this in mind, we recommend scheduling the backup of your Central Administration Site to run every day.

A couple of steps will enable you to recover as much of your central site as possible in the event of data loss:

- Back up the Central Administration Site every day.
- Have a reference site for the central site so that the restore process will be able to recover global data that is created after the site is backed up.

With these steps, you should be able to recover most of the Central Administration Site without too much trouble. You will be able to recover global and site data from the reference site.

Copying Site Backups to Another Location

The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager site system when it fails. The next time the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, because there will not be another backup to restore from.

For that reason, Microsoft recommends that you archive the backup to another location off the site server itself. As a best practice, it also recommends having multiple backup archives, for the following reasons:

- It is common for backup media to fail, get misplaced, or contain only a partial backup. Recovering a failed site from an older backup is better than recovering with no backup at all.
- A corruption in a site can go undetected for several backup cycles. You may need to go back several cycles to the backup snapshot from before the site became corrupted.
- The site might have no backup at all if, for example, the Backup ConfigMgr Site Server task fails. Because the backup task removes the previous backup snapshot before it starts to back up the current data, there will not be a valid backup snapshot.

Archiving the Backup Snapshot to Another Server with *AfterBackup.bat*

Microsoft has included support for a batch file appropriately called `AfterBackup.bat` to run tasks on the site server after the backup task is complete. After you successfully run the Backup

ConfigMgr Site Server maintenance task, ConfigMgr will try to run this batch file. This batch file is not installed during site setup and will have to be created manually by an administrator after a site server is configured and stored in `\Microsoft Configuration Manager\inboxes\smsbkup.box`.

If the `AfterBackup.bat` file exists and is stored in the correct folder on the site server, the batch file will run automatically once the backup task is complete. You can include commands in the `AfterBackup.bat` file that will archive the backup snapshot to a location off the server at the end of the backup operation and perform other post-backup tasks. The `AfterBackup.bat` file integrates the archive and backup operations, thus ensuring that every new backup is archived. If the batch file does not exist, it has no effect on the backup success, but in order to archive the backup snapshot, you must use another method.

Although the `AfterBackup.bat` file is intended to archive backup snapshots, you can include commands in that batch file that will run after every backup. As noted, the `AfterBackup.bat` file isn't created for you when ConfigMgr is installed, and the ConfigMgr documentation does not explain how to set up the `AfterBackup.bat` file to be able to accomplish this task.

There are several ways to do this (including using third-party tools), some more complicated than others, but probably the simplest way is to use the Windows command `robocopy`. As illustrated in Figure 18.2, a `robocopy` command will copy all files from `D:\CM2012.bck` to a network share called `\\File01\backup\CM01`.

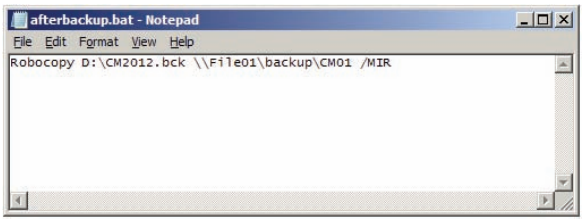


FIGURE 18.2 A sample `Afterbackup.bat` file

To create the `Afterbackup.bat` file, follow these simple steps:

1. Open Windows Explorer and navigate to `\Microsoft Configuration Manager\inboxes\smsbkup.box`.
2. Create a new ASCII batch file and name it **`AfterBackup.bat`**.
3. Type **`Robocopy D:\CM2012.bck \\File01\backup\CM01 /MIR`**.
4. Save and close the file.
5. Upon the next backup, open the `smsbkup.log` file and search for the text `Afterbackup.bat` to verify that the file has been executed.

One of the drawbacks of archiving this way is that the files will be copied over the network uncompressed to your remote file location. Depending on the size of your ConfigMgr database, archiving may take a long time and might use up a lot of bandwidth if your remote location is on a slow link. With that in mind, you can also add commands to the `AfterBackup.bat` file to use file compression software such as WinZip to compress the backup files before they are copied to the remote archive location.

Windows Application Log Entries Created by the Backup Process

The Backup ConfigMgr Site Server task will write backup status messages to the Application log in Windows event viewer. Table 18.1 shows a list of the events and their event IDs that are written to the Application log, as described in the Microsoft documentation. You will be able to intercept the events using a monitoring system like Microsoft System Center Operations Manager.

TABLE 18.1: Configuration Manager backup Application log entries

EVENT ID NUMBER	MESSAGE
3197	I/O is frozen on database CM_SiteCode. No user action is required. However, if I/O is not resumed promptly, you could cancel the backup.
3198	I/O was resumed on database CM_SiteCode. No user action is required.
5040	This event is used to indicate that the `AfterBackup.bat` file was successfully started.
5055	Component SMS_SITE_BACKUP on computer site server reported: Site Backup task is starting. This task will interact with the Windows VSS services and the appropriate writers to create a volume snapshot and then back up the required files to the specified destination.
5056	Component SMS_SITE_BACKUP on computer site server reported: Site Backup is starting to copy the files from the snapshot.
5057	Component SMS_SITE_BACKUP on computer site server reported: Site Backup has successfully completed copying the files from the snapshot.
6829	Component SMS_SITE_VSS_WRITER on computer CM03 reported: SMS Writer is about to stop the ConfigMgr Services as part of the preparation for the site backup.
6830	Component SMS_SITE_VSS_WRITER on computer site server reported: The snapshots of the volumes required for the Site Backup have been successfully created.
6831	Component SMS_SITE_VSS_WRITER on computer site server reported: SMS Writer has started the ConfigMgr Services successfully.
6833	Component SMS_SITE_BACKUP on computer site server reported: Site Backup has successfully completed copying the files from the snapshot.
18265	Database backed up.

Configuring the Backup ConfigMgr Site Server Maintenance Task

The Backup ConfigMgr Site Server maintenance task backs up a Configuration Manager site, including the site database, files, registry keys, and system configuration data. The site-recovery process does not support using third-party tools to back up your Configuration Manager site. If you are running Configuration Manager in a virtual environment, please note that taking snapshots of the site server is not a supported backup method and cannot replace using the site maintenance backup task, a SQL database backup, or a backup performed via Data Protection Manager. It is important to note that the Backup ConfigMgr Site Server maintenance task is not enabled by default and should be enabled during the initial configuration of the Configuration Manager site.

Backing Up a Site Server

To configure a daily backup do the following:

1. In the Configuration Manager console, navigate to the Administration workspace ➢ Overview ➢ Site Configuration ➢ Sites.
2. Select the site and choose Settings ➢ Site Maintenance from the ribbon.
3. Select the Backup Site Server task, and click Edit.
4. Select Enable This Task.
5. Click Set Paths and type the path for the backup folder.

   If you are logged on locally to the site server, you can click Browse and select a location; otherwise, you will have to manually type a path. Depending on the location of the SQL database, you will be given three choices for where to save the database and the backup files:

   - Local Drive On Site Server For Site Data And Database

     This option is available if the SQL database is hosted locally on the site server.

   - Network Path (UNC Name) For Site Data And Database

     This option will allow you to specify a network share to store the backup files.

   - Local Drives On Site Server And SQL Server

     This option is available only if you have SQL running on a remote server. The SQL database will be stored locally on the SQL Server separately from the site data.

   Regardless of what location you select, you need to ensure that the site server computer account has write access to the folder or share that is used to store the backup files. It is recommended to create the folder prior to running the backup task.
6. You can also modify the Start After and Latest Start Time settings if the default schedule interferes with other maintenance routines.
7. Select Enable Alerts For Backup Task Failures and click OK, as shown in Figure 18.3.

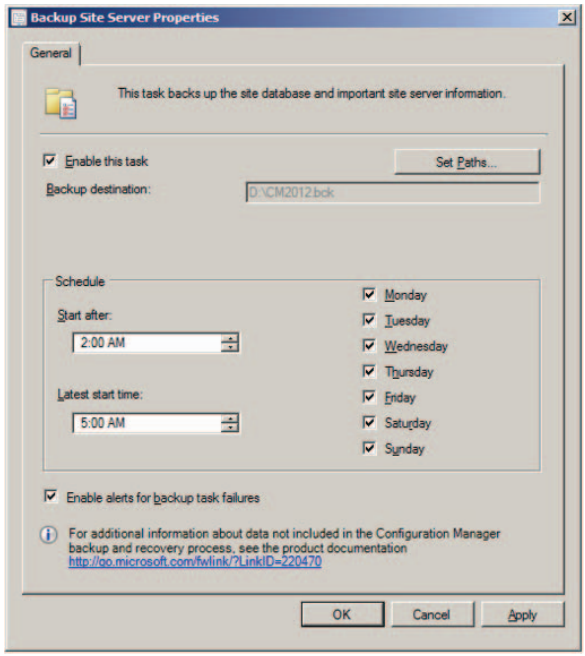


FIGURE 18.3
The Backup Site Server task

This will ensure a daily backup. The duration of the backup will vary from site to site, but by reading the `smsbkup.log` file or monitoring the events created in the viewer as described in Table 18.1, you will be able to tell the exact duration in your environment.

TESTING THE SITE BACKUP

As soon as you set up the backup maintenance task on a site, you should let it run and verify that it is running. That way, you won't be surprised to find yourself without a good backup if you have to restore one of your site servers.

To do this, follow these steps:

1. Log on to the site server.
2. Open a command prompt as administrator.
3. Type **`net start sms_site_backup`**, as shown in Figure 18.4; this will start the backup service and perform the first backup.

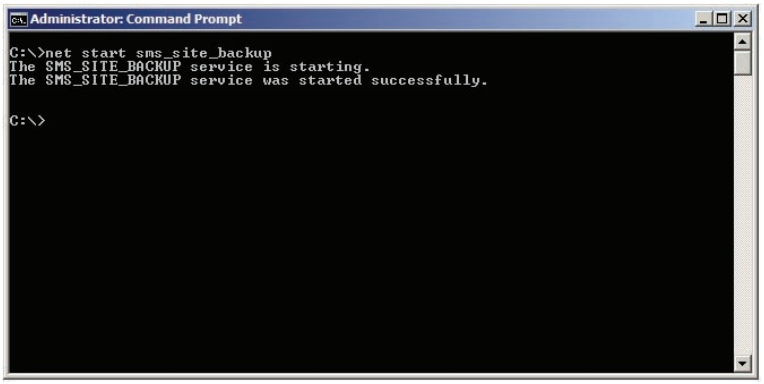


Figure 18.4
Manually starting the Backup Site Server task

4. Open CMTrace (formerly known as SMS Trace or Trace32) and monitor the `smsbkup.log` file from the `Logs` folder on the site server.

   The backup log file will give you valuable information about the process. By reading the log file you can calculate the backup duration, troubleshoot errors related to the process, and see if the `Afterbackup.bat` file started successfully.

Common Backup Troubleshooting Methods

If the previous tests don't help you figure out what is causing the problem with the backup, you can look for errors in a few additional places:

- Look in the Event Viewer logs for any account and/or access violations.
- The SMS_SITE_BACKUP runs under the local system account. Make sure that this account has access to any remote locations in the SMS Backup control file and that this account has the rights to perform the tasks in the control file's `[Tasks]` section.
- Check the `smsbkup.log` file for errors.

  You should be able to see a status message with the ID 5035 to indicate a successful backup. It can be found at *<Configuration Manager installation directory>*`\Logs\smsbkup.log`.
- Open the Alerts view in the Configuration Manager console and check the status of the alert titled "Site backup task failure alert at site."

Restoring Configuration Manager

Besides getting a failed site up and running again, recovery of a Configuration Manager site is also required if that site is installed with a site code or site server name that has already been used in the hierarchy. Repairing and resynchronizing data is what site recovery is designed for, and it is required in order to avoid interruption of operations and corruption of data.

Configuration Manager provides recovery and reset tools to help you quickly and consistently complete the tasks that are essential to restoring Configuration Manager site operations. These tools allow you to run recovery and reset commands that will override existing configuration settings without having to directly access low-level data, as well as to start operations that are not available through other methods.

Understanding the Effects of a Site Failure

Configuration Manager is made up of various site systems and clients. Each site has at least one site system—namely, the site server. The site server will monitor and manage the Configuration Manager site. Each Configuration Manager site also has a site system that is the site database server and at least one site system that acts as a management point. As already established in previous chapters, the management point is the site system that allows the site server and the site's clients to communicate properly.

Along with these important site systems, a site can have any number of additional site systems that perform different roles for a site hierarchy. If the site server or any of its site systems fail, then they would not be able to provide the services they normally do. If more than one site role is installed on the same server and it fails, then all the services provided by that server will become unavailable. Table 18.2 shows the results of various site systems going offline or otherwise becoming unavailable.

Table 18.2: Results of Configuration Manager site failure

Site Server	Site Database *	Management Point *	Distribution Point *	Result
Offline	Online	Online	Online	No site administration will be possible, including creation of new deployments. The management point will collect client information and cache it until the site server is back online. Existing deployments will run, and clients can find distribution points.
Online	Offline	Online	Online	No site administration will be possible, including creation of new deployments. If the Configuration Manager 2012 client already has a policy assignment with new policies and if the management point has cached the policy body, the client can make a policy body request and receive the policy body reply. No new policy assignment requests can be serviced. Clients will be able to run programs only if they have already been detected and the associated source files are already cached locally at the client.

Site Server	Site Database *	Management Point *	Distribution Point *	Result
Online	Online	Offline	Online	Although new deployments can be created, the clients will not receive them until a management point is online again. Clients will still collect inventory, software metering, and status information and store it locally until the management point is available. Clients will be able to run programs only if they have already been detected and the associated source files are already cached locally at the client.
Online	Online	Online	Offline	Configuration Manager 2012 clients will be able to run deployments only if the associated source files have already been downloaded locally.

** Note that you configure multiple management points and distribution points and cluster the SQL database. By doing so, you will minimize the risk of service breakdown in the event that one site system is unavailable.*

Recovering a Configuration Manager Site

Before starting a site restore you will need to know why you are performing the restore and what you are trying to achieve. If you experience data loss or a complete hardware failure, you will need to perform a site restore. But if you experience problems with some of the site server components, you might want to start with a site reset.

Unlike previous versions of Configuration Manager and SMS, there is no longer a specific Site Repair Wizard. Instead, the recovery process is offered as part of the standard installation process. When you start a Configuration Manager site installation, you will be given the option to recover a site, as shown in Figure 18.5.



Figure 18.5 Starting the site recovery process

If you do not see the Recover A Site option, first uninstall the site. Uninstalling a site is a straightforward process for a single site. If you want to uninstall a parent site in a multisite hierarchy, you will need to manually delete the site database first.



Real World Scenario

Preparing for a Site Restore on a Central Administration Site

As a Configuration Manager administrator for YNWA Inc., you have been asked to perform a complete site restore for the Central Administration Site, named CAS. You run the setup utility but notice that you do not have the option to recover the site. You then try running the site uninstall option, but it fails because the site has multiple child sites. You realize that you first need to delete the database. To do so, you follow these steps:

1. Log on to SQL Server.
2. From the Start menu, select All Programs ➢ Microsoft SQL Server.
3. Start SQL Server Management Studio.
4. Click New Query and enter the following query:

```
ALTER DATABASE CM_CAS
SET SINGLE_USER WITH ROLLBACK IMMEDIATE
Drop Database CM_CAS
```

5. Highlight the query statement and click Execute in the toolbar.
6. Close SQL Server Management Studio and restart the setup utility.

When you start the recovery process you will be given two site server recovery choices and four database recovery choices, as explained in Table 18.3

Table 18.3: Recovery options

Option	Used When
Recover This Site Server Using An Existing Backup	You have the backup files created using Configuration Manager. This offers you a complete recovery scenario, as described later in this chapter.
Reinstall The Site Server	You do not have a backup of the site server. All site settings will be lost, and you will have to manually reconfigure the site.
Recover The Site Database Using A Backup Set At The Following Location	You have a backup of the Configuration Manager site database. This offers you a complete recovery scenario, as described later in this chapter.
Create A New Database For This Site	You are recovering a site that is part of a hierarchy, and you want to replicate data from the Central Administration Site or from another reference site. Note that this option is available only in multisite environments. Depending on the size of the site database, this will generate a lot of WAN traffic.
Use A Site Database That Has Been Manually Recovered	You already have recovered the site database using a tool other than the one provided by Configuration Manager 2012.
Skip Database Recovery	You haven't experienced any data loss and the existing database is intact.

Recovering Configuration Manager

As mentioned earlier in this chapter, there are major differences between recovering a ConfigMgr 2012 site and a Configuration Manager 2007 site. Gone is the Site Repair Wizard; instead, you initiate the recovery process by running the site setup process. The process can be divided into two phases:

1. Reading the `ConfigMgrBackup.ini` file from the backup source
2. Running the setup process based on the information in the `ConfigMgrBackup.ini` file combined with user input in the recovery phase

Unlike previous versions of Configuration Manager and SMS, there is no need to run a site reset process manually after recovering the site because that is an integrated part of the recovery process.

How to Start a Recovery Process

The site recovery process is designed to make recovering a Configuration Manager site as easy as possible.

Before you start the recovery process, ensure that you have the following:

- The SQL installation media
- The Configuration Manager 2012 prerequisites
- The Configuration Manager 2012 installation media
- Access to the Configuration Manager 2012 site backup files

Furthermore, ensure that you use the following:

- Same site server name (it can be a different operating system)
- Same SQL Server name (it can be a different SQL version)
- Same site code
- Same database name
- Same Configuration Manager major version

To recover from a failed site you are given two options to start the process:

- Run *<Installation source>*`\SMSSETUP\BIN\X64\Setup.exe`, and select the Recover A Site Server option.
- Run an unattended installation of Configuration Manager using the `setup.exe /script` option.

Recovering a Central Administration Site

To restore the Central Administration Site using the setup process, do the following:

1. On the site server, open a command prompt with administrative privileges.
2. Navigate to `.\SMSSetup\BIN\X64\` in the Configuration Manager installation source and run `Setup.exe`.

3. Click Next in the Before You Begin page.
4. Select Recover A Site.
5. On the Site Server And Database Recovery Options page, click Browse, and select the location of the Configuration Manager backup files.
6. Select Recover This Site Server Using An Existing Backup.
7. Click Browse, and navigate to the location of the backup folder.
8. In the site database option, select Recover The Site Database Using The Backup Set At The Following Location.
9. Click Browse and navigate to the location of the backup folder.
10. Once you have selected the recovery options for the site and the database (see Figure 18.6), click Next.
11. On the Site Recovery Information page, shown in Figure 18.7, type the name of the site to reference and click Next.

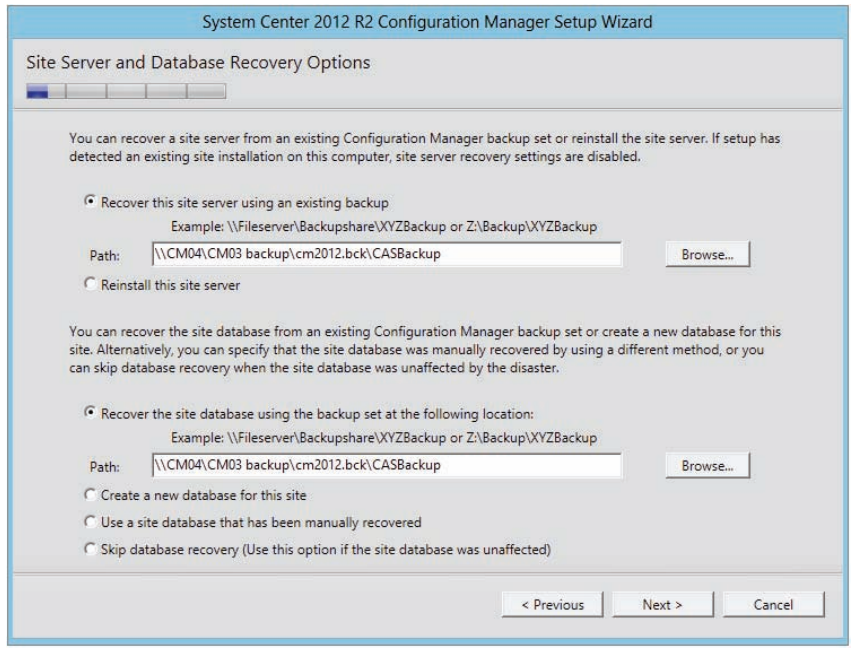
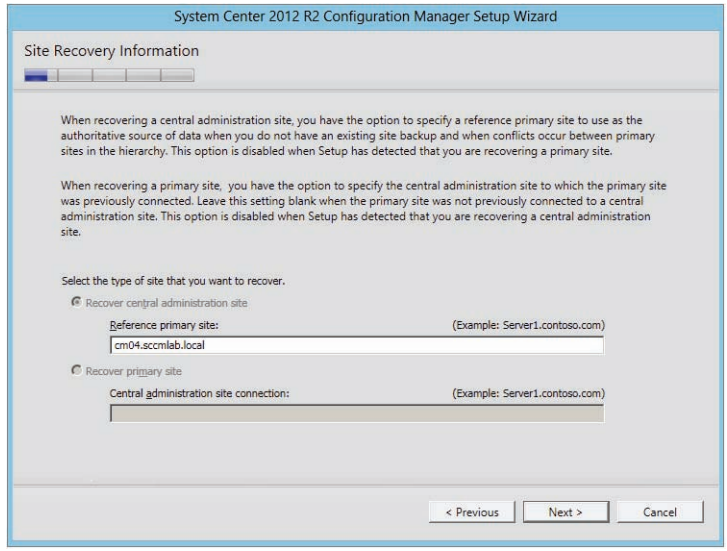


FIGURE 18.6
The Site Server And Database Recovery Options page

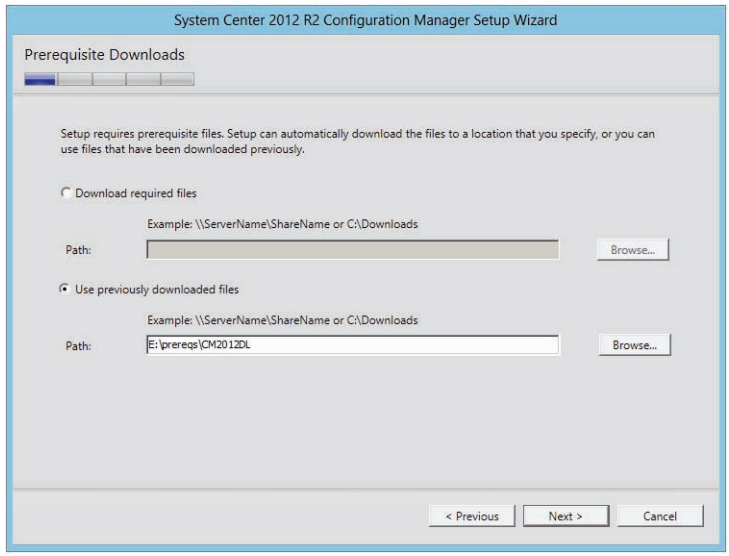
FIGURE 18.7
The Site Recovery Information page



The reference site will be used as the authoritative source in the recovery process. Data changes from other non-reference primary sites will be lost.

12. Accept the license terms and click Next.
13. On the Prerequisite Components page, shown in Figure 18.8, select Use Previously Downloaded Files.

FIGURE 18.8
The Prerequisite Components page



14. Click Browse, and select the location where you have the stored prerequisites.
15. On the Site And Installation Settings page, shown in Figure 18.9, modify the installation folder to reflect where you want to install Configuration Manager, and click Next.

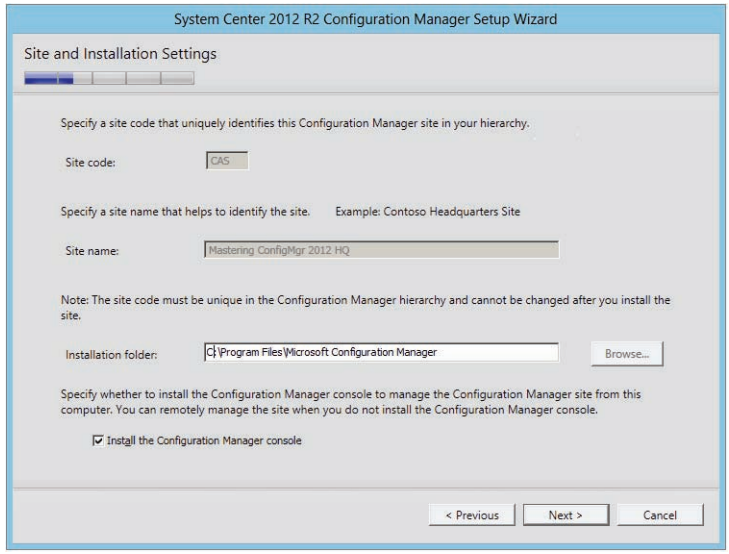


FIGURE 18.9
Site And Installation Settings page

16. On the Database Information page, shown in Figure 18.10, verify that the SQL Server Service Broker Port is correct, and click Next.

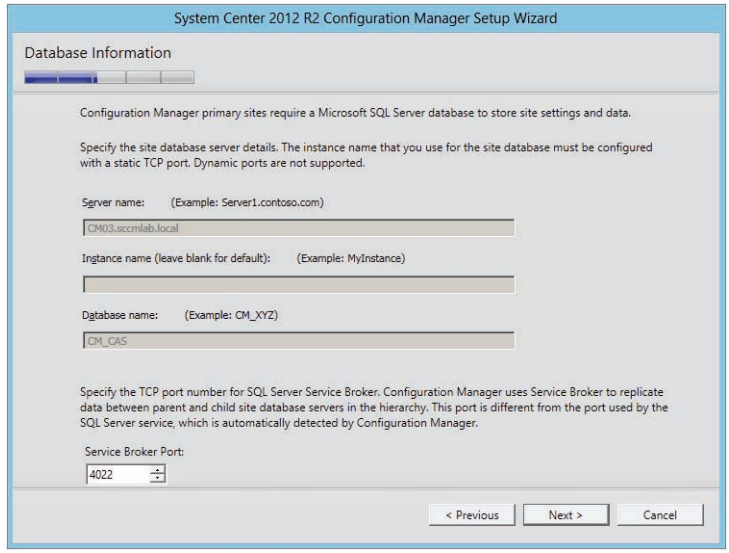
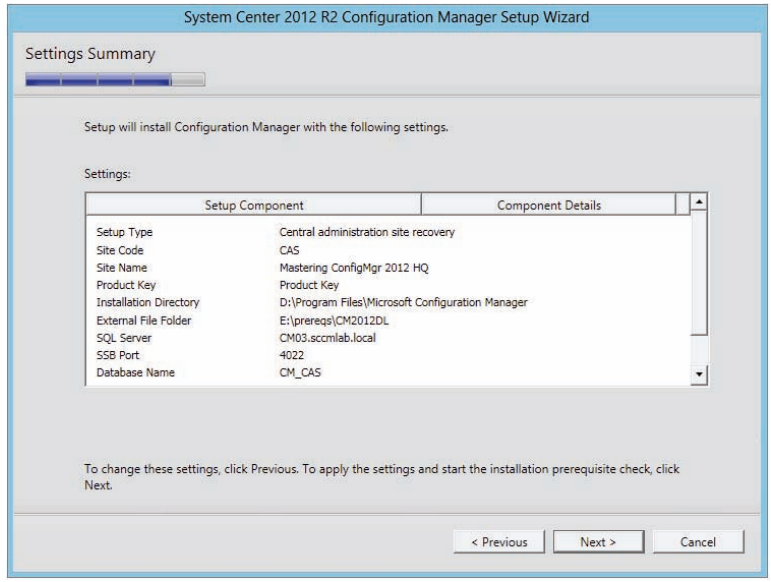


FIGURE 18.10
Database Information page

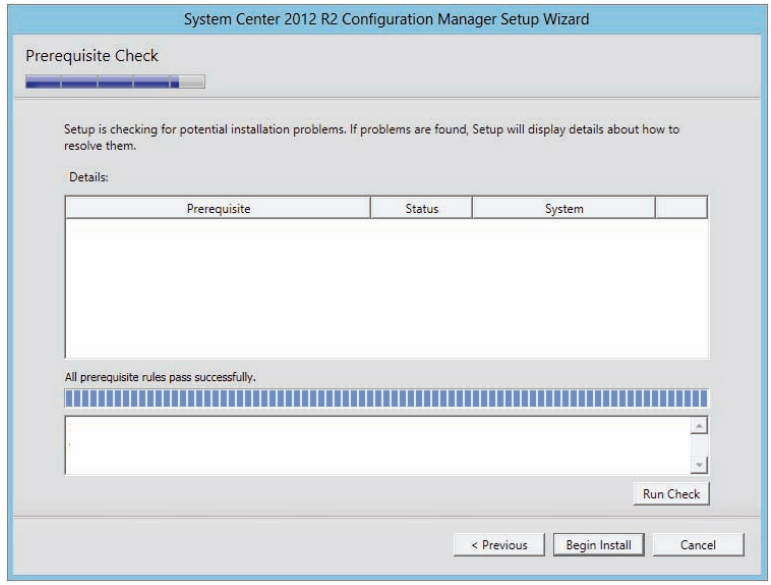
17. On the Settings Summary page, shown in Figure 18.11, review the information, and click Next if everything is correct.

FIGURE 18.11
Settings Summary page



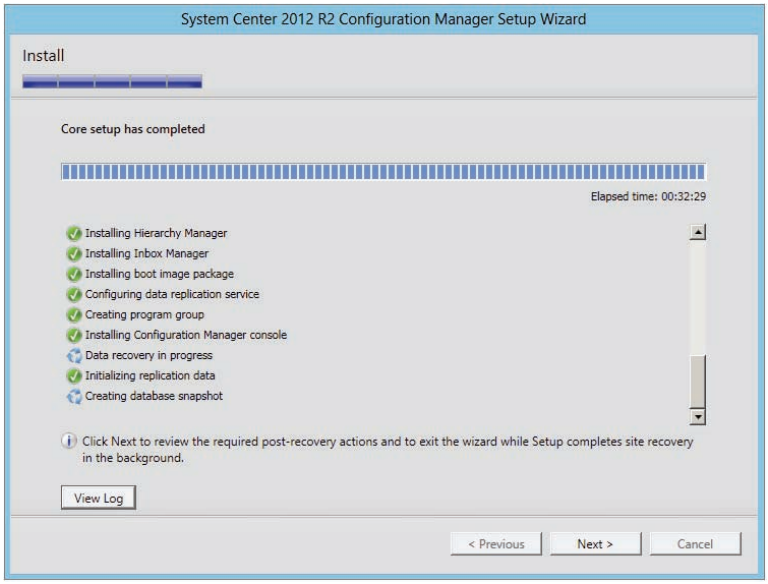
18. On the Prerequisite Check page, shown in Figure 18.12, ensure that all the prerequisites are met, and click Begin Install.

FIGURE 18.12
Prerequisite Check page



The installation and recovery process will require some time to finish. Once the process is finished, you will see the Install page, as shown in Figure 18.13.

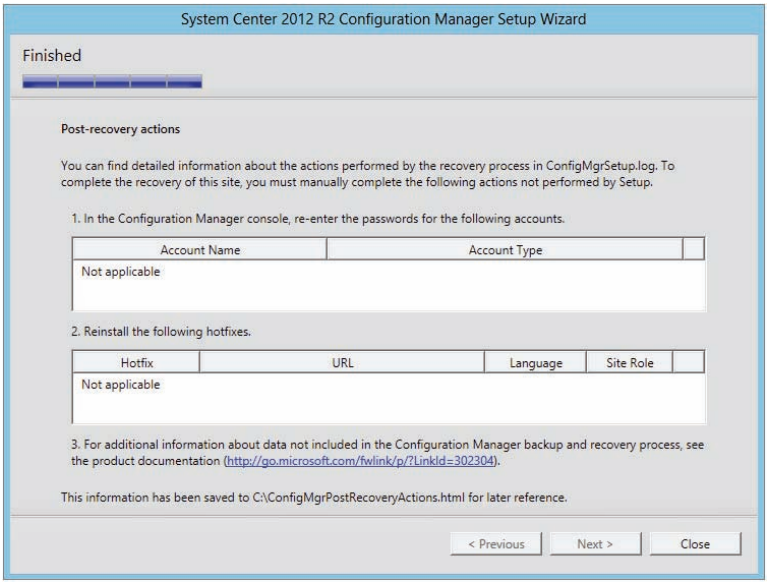
FIGURE 18.13
Install page



19. Review the page, and click Next.

The Finished page, shown in Figure 18.14, is the last page and explains the post-recovery tasks that you must perform.

FIGURE 18.14
Install page



20. Read the information and click Close.

After the recovery process and the global data has been replicated from the reference site, the CAS will go through these steps:

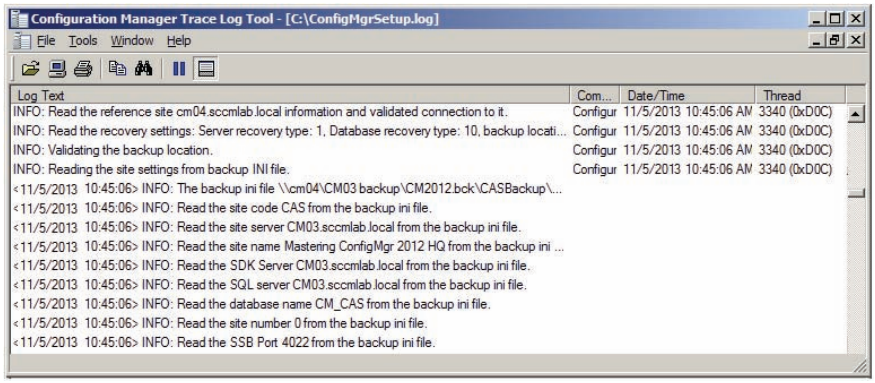
1. Recalculate IDs.
2. Reseed identity keys.
3. Initialize a site reset to reinstall the site components.
4. Generate public keys for child sites.

Monitoring the Recovery Process

You can monitor the process by following the Setup Wizard as it moves through the different setup steps. For a deeper dive into what's going on behind the scenes, you should open these log files:

`ConfigMgrSetupWizard.log` In this log file you will see how the backup process starts by reading the `ConfigMgrBackup.ini` file from the Configuration Manager backup folder. The information from the `.ini` file is used to configure some of the mandatory settings presented on the Site And Installation Settings page.

Figure 18.15 Verifying the recovery process



`ConfigMgrSetup.log` This is the main log file where you can find information about verifying the reference site and running the actual installation. Figure 18.15 illustrates that you can use the `ConfigMgrSetup.log` file to verify the recovery process.

Recovering a Primary Child Site

Recovering a primary child site is almost identical to recovering a Central Administration Site, except that the wizard automatically will configure the Central Administration Site as the reference site.

Recovering a Primary Standalone Site

Recovering a primary standalone site is almost identical to recovering a Central Administration Site, except that the wizard will not allow you to configure any reference sites during the setup process.

Recovering a Secondary Site

System Center 2012 Configuration Manager SP1 and R2 provide the ability to recover a secondary site server. The recovery of a secondary site may be necessary if the secondary site server fails. The recovered secondary site server must meet all of the prerequisite items for the installation of a secondary site and also must have the same configuration as the failed server, including the fully qualified domain name (FQDN) and the same installation path for the Configuration Manager binary files. The Configuration Manager primary site will reinitialize the data that is required on the secondary site as part of the recovery process. If the content library still exists on the secondary site server, Configuration Manager will verify that the library is valid and utilize it. If the content library does not exist, you will need to redistribute or prestage the content to the secondary site server. You can distribute the compressed packages using USB or similar media to the remote location. At the remote distribution point, run `ExtractContent.exe` found in the `SMS_DP$\SMS\Tools` folder on the remote distribution point.

Note: During a secondary site recovery, Configuration Manager will not install SQL Server Express if it is not installed on the server being recovered. You will need to manually install SQL Server Express. If you chose to utilize Microsoft SQL Server as the database component for the secondary site, you will need to install SQL Server and ensure that the same version of SQL is being used as well as the same instance name.

Recovery Scenarios for Multisite Environments

In a multisite environment you might come across different recovery scenarios where data might be recovered from another site in the hierarchy or might be lost. Let's look at three different scenarios. Common for all three scenarios is that you create an application with a single revision, perform a backup, and after that, modify that same application with revision 2. That way the current backup contains only revision 1.

Environment	Scenario	Revision after Recovery
One primary site with a secondary child site	Global data about the application with revision 1 being replicated to the secondary site.	1
One CAS with two primary sites (PS1 and PS2)	You create revision 2 on PS1, after which revision 2 is replicated to the CAS and PS2. PS1 fails and is recovered from backup.	2 PS1 will recover revision 1 from backup but will update to revision 2 after synchronizing with the CAS.
One CAS with two primary sites (PS1 and PS2)	You create revision 2 on PS1, after which PS1 fails before synchronizing any global data and is recovered from backup.	1 PS1 will recover revision 1 from backup and revision 2 will be lost.

Unattended Recovery of a Site

Configuration Manager 2012 supports recovering a Central Administration Site and a primary site via the Setup Wizard. You can also recover these sites via an unattended recovery script.

In order to use the unattended recovery solution you will need to create the `.INI` file that will be read by the `Setup.exe` application. The name of the file is not important, but the file extension must be `.INI`. You will run the Configuration Manager `Setup` command and reference the unattended script file in the command-line syntax. For example, if your unattended recovery script is named `ConfigMgrUnattendRecoverCAS.ini` and is located on the `C:` drive in the `CMRECOVERY` folder, the command will be `Setup.exe /script C:\CMRECOVERY\ConfigMgrUnattendCAS.ini`. The account used to execute `Setup.exe` must have administrator rights, so you may need to open a command prompt as an administrator and then run `Setup.exe` from there.

The `.INI` file you create will provide the same information that would be required as if you were performing a site recovery via the Setup Wizard. One key difference is that no default settings are applied in the unattended scenario, and as a result, all values for the recovery process must be specified in the script file.

The information that is required in the `.INI` file will depend on the recovery scenario. Also, the keys in the file are not case sensitive, and when you provide values for keys you must use an equals sign to separate the key from the value. The TechNet article "Unattended Site Recovery Script File Keys" at `http://technet.microsoft.com/en-us/library/gg712697.aspx#BKMK_UnattendedSiteRecoveryKeys` documents the available keys that can be used in the `.INI` file.

Other Site Maintenance Options

Besides doing a full recovery you can start other maintenance options by running Configuration Manager Setup from the Start menu. Those options are explained in Table 18.4.

Table 18.4: Site reset and maintenance options

Option	Used When
Reset Site With No Configuration Changes	You want to perform a site reset. During the site reset, all site components are reinstalled, and permissions and registry keys are restored to their default settings.
Modify SQL Server Configuration	You want to move the site database to another SQL Server. Note that this process requires that you have already copied the SQL database to the new SQL Server. The process will not detach the database from the old location or attach it to the new server. The process also allows you to modify the SQL Service broker port.
Modify SMS Provider Information	You want to install the SMS provider on another server.
Modify Language Configurations	You want to add new server and client languages to the installation.

The Hierarchy Maintenance Tool

The Hierarchy Maintenance tool (`preinst.exe`) is a command-line tool that you may need to use to diagnose problems with a site system, help repair a site, shut down site systems, or do other maintenance tasks that, for whatever reason, can't be performed using the Configuration Manager console. This tool must be run locally on the site server computer.

To use the Hierarchy Maintenance tool, do the following:

1. Open a command prompt window with administrative privileges.
2. Navigate to the location of `preinst.exe`, which by default is

   <drive where ConfigMgr is installed>`\Microsoft Configuration Manager\bin\x64\`*<language code>*

   The language code for English is 00000409.
3. Once you are there, just type **`preinst.exe`** to get a list of command-line options.
4. Then use `preinst.exe` with its command-line options, listed in Table 18.5 (adapted from Microsoft documentation), to complete your task.

TABLE 18.5: Hierarchy Maintenance tool syntax

COMMAND	DESCRIPTION
`/dump` *<site code>*	This command writes site control images to the root of the folder of the drive where the site is installed. `/dump` *<site code>* writes the site control file of only the site specified. `/dump` writes the site control files for all sites.
`/deljob` *<site code>*	This command deletes all jobs targeted to the site you specify in the command line.
`/delsite` *<site code>*	This command deletes child sites that were not previously removed successfully from the site database of its parent site.
`/stopsite`	This command shuts down the Configuration Manager 2012 Site Component Manager service, which will partially reset the site. When this shutdown is finished, ConfigMgr services on a site server and its remote systems are stopped. These services are flagged for reinstall, and some passwords are automatically changed when these services are reinstalled. When the shutdown cycle is started, it automatically runs and skips any computers or components that are not responding. If the Site Component Manager service can't access a remote site system during this process, the components on the remote site system will be reinstalled when the Site Component Manager service is restarted. This will continue until Site Component Manager succeeds in reinstalling all services that are marked for reinstallation. You can restart the Site Component Manager service using Service Manager just like other Windows services. After you use the `/stopsite` command to start a shutdown cycle, there is nothing you can do to stop the subsequent reinstall cycles when the Site Component Manager service is restarted. You can monitor the effect of the process by reading the `sitecomp.log` file on the site server.
`/keyforparent`	This command is run on sites that you are trying to recover after failure and is used to distribute the new public key to a parent site of the failed site. The `/keyforparent` command places the public key of the failed site in the file *<site code>*`.CT4` at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the parent site's `hman.box` inbox (not in the `pubkey` folder).

Command	Description
/keyforchild	This command is run on sites that you are trying to recover after failure and is used to distribute the new public key to a child site of the failed site. The /keyforchild command places the public key of the failed site in the file *<site code>*.CT6 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the child site's hman.box inbox (not in the pubkey folder).
/childkeys	This command is run on the recovering site's child sites and is used to distribute public keys from all child sites to the recovering site. The /childkeys command places this and all child site public keys into the file *<site code>*.CT6 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the parent site's hman.box inbox.
/parentkeys	This command is run on the recovering site's parent site and is used to distribute public keys from all parent sites to the recovering site. The /parentkeys command places this and all parent site public keys into the file *<site code>*.CT7 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the child site's hman.box inbox.

Post-Recovery Tasks

After you recover a site, there are tasks that you should perform to make sure that the site has been properly repaired and is functioning correctly:

- Monitor site processes.
- Verify site setting configuration.
- Re-enter user passwords.

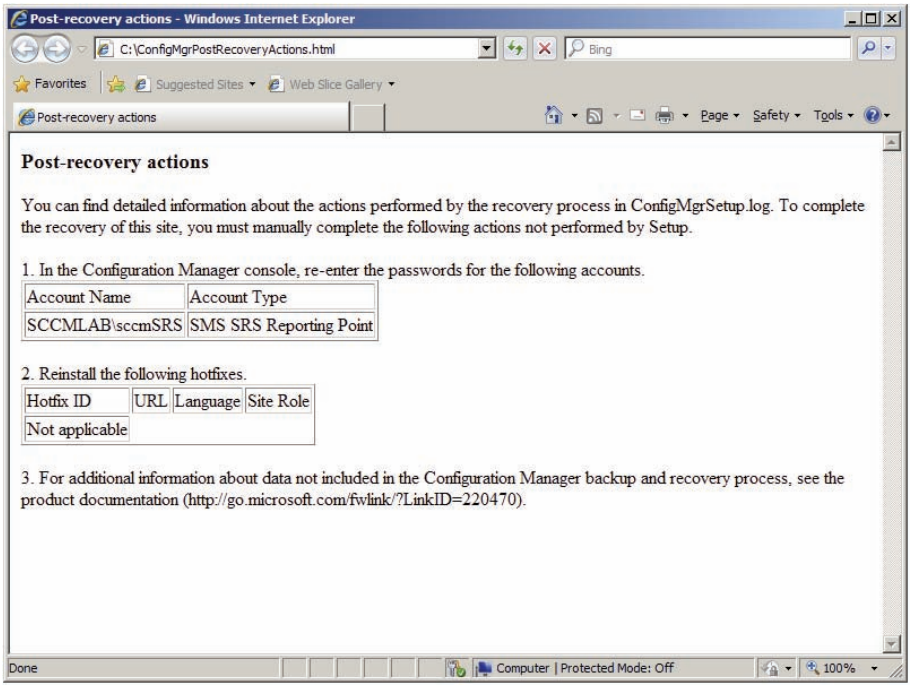
  All user passwords will be reset during the recovery process. You can find a list of affected user accounts in the C:\ConfigMgrPostRecoveryActions.html file, as shown in Figure 18.16.

- Reinstall previously applied hotfixes.

  You can find a list of installed hotfixes in the C:\ConfigMgrPostRecoveryActions.html file.

- Verify that the content library is fully rebuilt from the original data sources. If you need to determine the package source location, you can run the SQL query SELECT * FROM V_PACKAGE command against the Configuration Manager database in Microsoft SQL Server to list the package properties.
- Recover any custom reports.

FIGURE 18.16
The `C:\ConfigMgrPostRecoveryActions.html` file



- Recover the SCUP 2011 database if that was affected. This is done by copying the database file.
- If the IIS server was configured to utilize HTTPS, you will need to reconfigure IIS to use the web server certificate.
- Reprovision previously provisioned Intel AMT computers.

  This requires that you request the AMT provisioning certificate again and reconfigure the passwords for the MEBx, AMT Provisioning Removal, and AMT Provisioning and Discovery accounts.
- Recover the MDT.
- The content stored in the user state migration data folders is not backed up by Configuration Manager and should be backed up and restored via an enterprise backup process.
- If cloud distribution points are being used, you will need to update the certificate. Refer to the Microsoft TechNet article "Planning for Content Management in Configuration Manager" at `http://technet.microsoft.com/en-us/library/b2516212-e524-4031-9a1f-7b768084304d#BKMK_CloudDPCerts`.



Real World Scenario

Moving the Site Database

As a Configuration Manager administrator for YNWA Inc., you have been asked to move the site database and log files named `CM_PS1` stored in `D:\SQLDB` and `E:\SQLLogs` from SQL1 to a new SQL Server on SQL2. Configuration Manager 2012 is installed on CM01. The new SQL Server is installed and is using the same collation configuration as the old server and the same disk layout. To move the database and log files, follow these steps:

1. Log on to CM01.
2. Open a command prompt with administrative privileges and navigate to *<configuration manager install dir>*`\ SMS\bin\x64\`*<language code>*.
3. Run `preinst.exe /stopsite`, and wait until all components and services have been successfully stopped.
4. Still in the command prompt, type **`Net stop ccmexec`** to stop the management point service.
5. Log on to the old SQL Server, Server1.
6. From the Start menu, select All Programs ➢ Microsoft SQL Server.
7. Start SQL Server Management Studio.
8. Click New Query, and type

```
use master
go
sp_detach_db 'CM_PS1'
go
```

9. Highlight the query statement, and click Execute in the toolbar.
10. Copy the database and log files to the new SQL Server.
11. Log on to the new SQL Server, Server2.
12. From Start, select All Programs ➢ Microsoft SQL Server.
13. Start SQL Server Management Studio.
14. Click New Query, and type

```
use master
go
sp_attach_db 'CM_PS1','D:\SQLDB\CM_PS1.MDF','E:\SQLlogs\CM_PS1_Log.LDF'
go
```

15. Log on to CM01, and open a command prompt with administrative privileges.
16. Navigate to *<configuration manager install dir>*`\ Microsoft Configuration Manager\bin\x64` and run `Setup.exe`.
17. Select Perform Site Maintenance Or Reset This Site, as shown in the following graphic, and click Next.
18. Select Modify SQL Configuration, and click Next.



19. In the Server Name field type **Server2** and click Next.

20. Once the SQL process is finished, close the wizard by clicking Close.

21. Restart the CM01 server.

The Bottom Line

Configure backups for Configuration Manager sites. Backing up Configuration Manager sites can be automated by scheduling the Backup ConfigMgr Site Server maintenance task. When the Configuration Manager backup service (SMS_SITE_BACKUP) starts, it uses instructions in the backup control file, located at

```
[ConfigMgr Install Location]Microsoft Configuration Manager\Inboxes\
smsbkup.box\smsbkup.ctl
```

Master It Recovering a complete Configuration Manager site is only supported with site backups from what source?

Recover Configuration Manager sites. Recovery of a Configuration Manager site requires that you do not have a Configuration Manager site installed when starting the `Setup.exe` process. The recovery process will recover data from the backup files and from a reference site provided you have a multisite hierarchy.

Master It What is site recovery designed for?

Archive backup snapshots to another location. The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager site system when it fails. The next time the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, because there is no other backup to restore from.

Master It What script can you use to copy backup snapshots from the site server to a new location but is not created when ConfigMgr is installed?

Reinstall the site components and reset file and registry permissions to their default settings. From time to time other administrators mess around with the default permissions that are configured on the different folders and shares created by Configuration Manager.

Master It How can you restore the file and registry permissions without performing a complete restore?



Chapter 19

Troubleshooting

So far you have read about various aspects of Configuration Manager 2012 R2, and in each chapter we have explained different aspects of the product and have assumed that every component will work correctly. However, everyone knows that situations may occur with the product that require troubleshooting, and every IT professional needs to know how to identify the problem and find a possible solution. There are many resources online that can assist you in this process; some of these places are Microsoft TechNet, Bing, and MVP blogs.

In this chapter, we will cover the basics of troubleshooting a ConfigMgr 2012 infrastructure and determining which log file you should look at first when a problem arises.

In this chapter, you will learn to

- Create a basic maintenance plan
- View log files using CMTrace
- Troubleshoot DRS replication
- Master the troubleshooting steps

Creating the Maintenance Plan

The best way to prevent issues from arising in Configuration Manager 2012 is to create and follow a standard maintenance plan. A well-executed maintenance plan allows administrators to be actively aware of their ConfigMgr 2012 hierarchy, offering a better chance of finding possible concerns before they become issues. Proactively watching the environment can reduce the number of major issues and thus keep your environment healthier.

ConfigMgr 2012 has some predefined site maintenance tasks that are enabled by default and some that need to be enabled. To view and modify the site maintenance tasks, take the following steps:

1. Open the ConfigMgr console, and choose the Administration workspace.
2. Expand Overview ➢ Site Configuration ➢ Sites, and select Site Name.
3. Right-click, browse to Site Maintenance, and click it to open the Site Maintenance window.

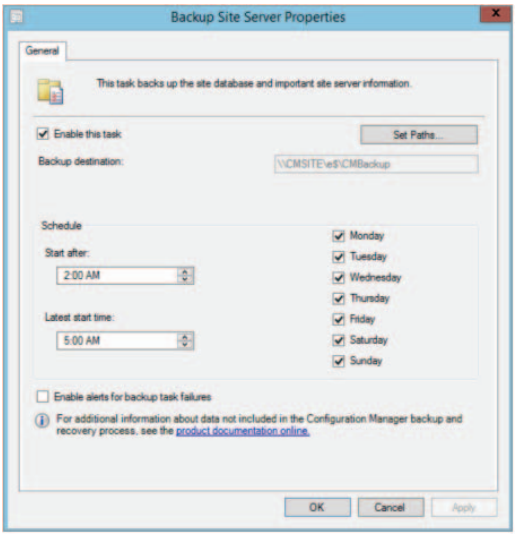
By default, Microsoft has 14 predefined tasks for the CAS server and 37 predefined tasks for primary sites. Secondary sites have only 4 predefined tasks. Some of these predefined tasks are enabled, while others are disabled by default.

4. To enable a task, select its name and click Edit to display the task's Properties dialog box.

   Figure 19.1 shows the Properties dialog box for the Backup Site Server task.

5. Select Enable This Task.

FIGURE 19.1
Enabling the Backup Site Server task in its Properties dialog box



SECONDARY SITES

You can back up a Central Administration Site and primary site, but there is no backup support for secondary sites or site system servers.

To ensure the proper health of the site, you should enable some of the predefined site maintenance tasks provided by Microsoft, and you'll need to modify the schedule of other tasks. Table 19.1 lists how the tasks should be configured in a typical maintenance plan; this might not be appropriate for all environments, but you can use the table as a guide.

Table 19.1: Site maintenance tasks

Task Name	Enabled by Default?	Schedule	Site Level
Backup Site Server	No	Daily	CAS/Primary
Check Application Title with Inventory Information	Yes	Weekly	CAS
Clear Install Flag	No	Weekly	Primary
Delete Aged Application Request Data	Yes	Daily	Primary
Delete Aged Client Operations	Yes	Daily	CAS/Primary
Delete Aged Client Presence History	Yes	Daily	CAS/Primary
Delete Aged Collected Files	Yes	Weekly	Primary
Delete Aged Computer Association Data	Yes	Weekly	Primary
Delete Aged Delete Detection Data	Yes	Daily	CAS/Primary
Delete Aged Device Wipe Record	Yes	Weekly	Primary
Delete Aged Devices Managed by the Exchange Server Connector	Yes	Weekly	Primary
Delete Aged Discovery Data	Yes	Weekly	Primary
Delete Aged Distribution Point Usage Data	Yes	Daily	CAS/Primary
Delete Aged Endpoint Protection Health Status History Data	Yes	Weekly	Primary
Delete Aged Enrolled Devices	Yes	Weekly	Primary
Delete Aged Inventory History	Yes	Weekly	Primary
Delete Aged Log Data	Yes	Daily	CAS/Primary/Secondary
Delete Aged Notification Task History	Yes	Daily	Primary
Delete Aged Replication Summary Data	Yes	Daily	CAS/Primary/Secondary
Delete Aged Replication Tracking Data	Yes	Daily	CAS/Primary/Secondary
Delete Aged Software Metering Data	Yes	Daily	Primary
Delete Aged Software Metering Summary Data	Yes	Weekly	Primary

TABLE 19.1: Site maintenance tasks *(CONTINUED)*

TASK NAME	ENABLED BY DEFAULT?	SCHEDULE	SITE LEVEL
Delete Aged Status Messages	Yes	Daily	CAS/Primary
Delete Aged Threat Data	Yes	Weekly	Primary
Delete Aged Unknown Computers	Yes	Weekly	Primary
Delete Aged User Device Affinity Data	Yes	Weekly	Primary
Delete Inactive Client Discovery Data	Yes	Weekly	Primary
Delete Obsolete Alerts	Yes	Daily	CAS/Primary
Delete Obsolete Client Discovery Data	Yes	Weekly	Primary
Delete Obsolete Forest Discovery Sites and Subnets	Yes	Weekly	CAS/Primary
Delete Unused Applications Revisions	Yes	Daily	Primary
Evaluate Provisioned AMT Computer Certificates	Yes	Weekly	Primary
Monitor Keys	Yes	Weekly	CAS/Primary
Rebuild Indexes	No	Weekly	CAS/Primary/Secondary
Summarize Installed Software Data	Yes	Weekly	Primary
Summarize Software Metering File Usage Data	Yes	Daily	Primary
Summarize Software Metering Monthly Usage Data	Yes	Daily	Primary
Update Application Catalog Tables	Yes	Intervals	Primary

Some tasks do not need to be performed as frequently as others, but it's important to develop a maintenance plan for them to ensure the proper health of the site.

Table 19.2 summarizes what a typical maintenance plan should be for ConfigMgr 2012. Again, these recommendations might not be appropriate for organizations of all sizes; the table is meant to be used only as a guide.

TABLE 19.2: Maintenance plan

TASK	INTERVAL	COMMENTS
Check status messages.	Daily	Check for warnings and errors. They are available in either a web report or within the administrative console.
Check event log on site server for warnings or errors.	Daily	This is the Windows event log.
Check log folders for crash dumps.	Daily	This will help you know whether the site system failed.
Monitor site system's inbox folder(s).	Daily	Check this for possible backlogs of files.
Clean out old machines and user accounts.	Daily	Remove old resources.
Check client status.	Daily	
Back up site server to removable media.	Daily	Ensure that the copy of the site backup is moved to removable media such as tape.
Delete unnecessary objects.	Weekly	Remove unneeded collections, packages, programs, advertisements, and queries.
Delete unnecessary files from site systems.	Weekly	Delete unneeded files.
Check disk space on all site systems.	Weekly	
Defragment all site systems.	Monthly	This can improve site performance.
Review site boundaries.	Quarterly	Ensure that your site boundaries are still valid.
Perform DR test.	Biannually	Ensure that backups actually work.
Review documentation.	Biannually	Confirm that documentation is updated and complete.
Review maintenance plan.	Biannually	Modify the maintenance plan if anything has changed or needs to be added or removed.

Getting an approved maintenance plan for your hierarchy is your first step to developing a solid ConfigMgr infrastructure. The next step is to automate as many of the tasks as possible so they can be done in the most efficient manner without sacrificing the results. A maintenance plan is only as strong as the people implementing the plan.

Using Troubleshooting Tools

The most important troubleshooting tools are log files and status messages. Getting to know the most common log files for ConfigMgr is the first step in identifying a potential situation on your site servers; you can also use this proactively to monitor your site server activity and to know what is being processed in your environment. That being said, let's take a look at the most common log files.

Log Files

For the majority of troubleshooting, administrators will focus on the log (`.log`) files on either the client or the server and in some cases both. The client stores the log files in the folder `C:\Windows\ccm\logs`, while the site server stores the log files in the folder *`<installation Directory>`*`\Microsoft Configuration Manager\Logs`. Table 19.3 lists site server log files, Table 19.4 lists management point log files, and Table 19.5 lists client log files.

The default location for the management point log files is `Program Files\SMS_CCM\Logs` on the management point.

TABLE 19.3: Site server and site system server log files

LOG FILE	PURPOSE
`Ccm`	Records client ConfigMgr tasks
`Cidm`	Records changes to the client settings by the Client Install Data Manager (CIDM)
`Colleval`	Logs when collections are created, changed, and deleted by the Collection Evaluator
`Compsumm`	Records Component Status Summarizer tasks
`Dataldr`	Processes management information format (MIF) files and hardware inventory in the ConfigMgr 2012 database
`Ddm`	Saves Discovery Data Record (DDR) information to the ConfigMgr 2012 database by the Discovery Data Manager
`Despool`	Records incoming site-to-site communication transfers
`Distmgr`	Records package creation, compression, delta replication, and information updates
`Hman`	Records site configuration changes and publishes site information in Active Directory Domain Services
`Inboxast`	Records files that are moved from the management point to the corresponding `INBOXES` folder
`Inboxmgr`	Records file maintenance
`Invproc`	Records the processing of delta MIF files for the Dataloader component for client inventory files

Log File	Purpose
Mpcontrol	Records the registration of the management point with WINS and records the availability of the management point every 10 minutes
Mpfdm	Management point component that moves client files to the corresponding INBOXES folder
Mpmsi	Management point .msi installation log
Mpsetup	Records the management point installation wrapper process
Offermgr	Records advertisement updates
Offersum	Records summarization of advertisement status messages
Policypv	Records updates to the client policies to reflect changes to client settings or advertisements
Replmgr	Records the replication of files between the site server components and the scheduler component
Schedule	Records details about site-to-site job and file replication
Sender	Records the files that transfer by file-based replication between sites
Sinvproc	Records client software inventory data processing to the site database in Microsoft SQL Server
Sitecomp	Records maintenance of the installed site components
Sitectrl	Records site setting changes to the Sitectrl.ct0 file
Sitestat	Records the monitoring process of all site systems
Smsdbmon	Records database changes
Smsexec	Records processing of all site server component threads
Smsprov	Records WMI provider access to the site database
Statmgr	Writes all status messages to the database
Swmproc	Processes metering files and maintains settings
Adctr	Records enrollment processing activity
ADForestDisc	Records Active Directory Forest Discovery actions
ADService	Records account creating and security group detail in Active Directory
Adsgdis	Records Active Directory Security Group Discovery actions

TABLE 19.3: Site server and site system server log files *(CONTINUED)*

Log File	Purpose
Adsysdis	Records Active Directory System Discovery actions
Adusrdis	Records Active Directory User Discovery actions
CertMgr	Records the certificate activities for intra-site communications
Chmgr	Records activities of the client health manager
Compmon	Records the status of component threads monitored for the site server
ComReqSetup	Records the initial installation of COM registration results for a site server
ConfigMgrPrereq	Records prerequisite component evaluation and installation activities
EPCtrlMgr	Records information about the synchronization of malware threat information from the endpoint protection site system role into the ConfigMgr database
EPMgr	Records the status of the endpoint protection site system role
EnrollSrv	Records activities of the enrollment service process
EnrollWeb	Records activities of the enrollment website process
Migmctrl	Records information for migration actions involving migration jobs, shared distribution points, and distribution point upgrades

TABLE 19.4: Management point log files

Management Point Log File	Purpose
MP_Ddr	Records the conversion of XML.ddr records from clients and copies them to the site server
MP_GetAuth	Records the status of the site management points
MP_GetPolicy	Records policy information
MP_Hinv	Converts XML hardware inventory records from clients and copies the files to the site server
MP_Location	Records Location Manager tasks
MP_Policy	Records policy communication
MP_Relay	Copies files that are collected from the client
MP_Retry	Records the hardware inventory retry processes

Management Point Log File	Purpose
MP_Sinv	Converts XML hardware inventory records from clients and copies them to the site server
MP_Status	Converts XML.svf status message files from clients and copies them to the site server
MP_CliReq	Records the client registration activity processed by the management point
MP_Framework	Records the activities of the core management point and client framework components
MP_OOBMgr	Records the management point activities related to receiving
MP_SinvCollFile	Records details about file collection

Table 19.5: Client log files

Client Log File	Purpose
CAS	Content Access Service for the local machine's package cache
CcmExec	Tracks the clients activities and SMS agent host service information
CertificateMaintenance	Records Active Directory certificates for the directory service and management points
ClientIDManagerStartup	Used for the maintenance of the resource's GUID
ClientLocation	Tracks the resource's site assignments
ContentTransferManager	Records scheduling information for the Background Intelligence Transfer Service (BITS) or Server Message Block (SMB) to download or to access ConfigMgr packages
DataTransferService	Records all BITS communication for policy or package access
Execmgr	Records advertisement information as advertisements execute
FileBITS	Records SMB package access tasks
InventoryAgent	Creates DDRs and hardware and software inventory records
LocationServices	Identifies located management points and distribution points
MIFProvider	Identifies the MIF WMI provider
Mtrmgr	Tracks software-metering processes
PolicyAgent	Requests policies by using the data transfer service

TABLE 19.5: Client log files *(CONTINUED)*

Client Log File	Purpose
PolicyAgentProvider	Records any policy changes
PolicyEvaluator	Records any new policy settings
Scheduler	Records schedule tasks for all client operations
SMSCliui	Records usage of the Systems Management tool in Control Panel
StatusAgent	Logs status messages that are created by the client components
SWMTRReportGen	Generates a usage data report that is collected by the metering agent
EndpointProtectionAgent	Records details about the installation of the Endpoint Protection client and the application of antimalware policy to that client

There are also log files outside ConfigMgr 2012 that you will need to be aware of when troubleshooting issues within Configuration Manager; Table 19.6 lists them.

TABLE 19.6: Additional log files

Name or Category	Location	Description
IIS log files	%windir%\system32\Logsfiles	Log file for Internet Information Services (IIS). Logs HTTP transactions.
SQL log files	SQL Enterprise Manager	Logs SQL activities.
WMI	%windir%\system32\wbem\logs	The WMI repository is the key to the hardware inventory of the clients. Become very familiar with these logs.

There are many more log files for each ConfigMgr component. To learn more about the rest of the log files you can check out the ConfigMgr 2012 Library at `http://technet.microsoft.com/en-us/library/hh427342.aspx`. Here you can find details including the log file location and descriptions. Since ConfigMgr has many log files, we point out only the most common ones in this chapter.

The best tool for reading log files we have seen is CMTrace, a log viewer that constantly monitors the opened file for updates. You can find CMTrace in the `SMSSETUP\Tools` folder on the ConfigMgr 2012 R2 source media. It provides real-time updates of any log file, allowing administrators to see exactly what is happening on a client or site system. If that isn't enough to win you over, CMTrace includes the capability to highlight and filter features to allow at-a-glance log viewing. Finally, the tool includes an error code dictionary, shown in Figure 19.2, so that you can quickly translate most of Microsoft's decimal error codes into useful information right within the tool. For example, entering 5 in the Error Lookup window returns "Access Denied." This feature is available by selecting Tools ➢ Lookup in the CMTrace utility. CMTrace will highlight errors, as shown in Figure 19.3, so they stand out.

FIGURE 19.2
CMTrace Error Lookup window

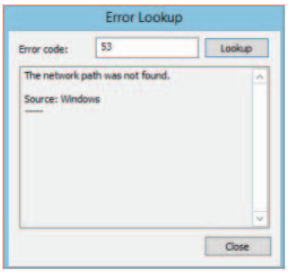
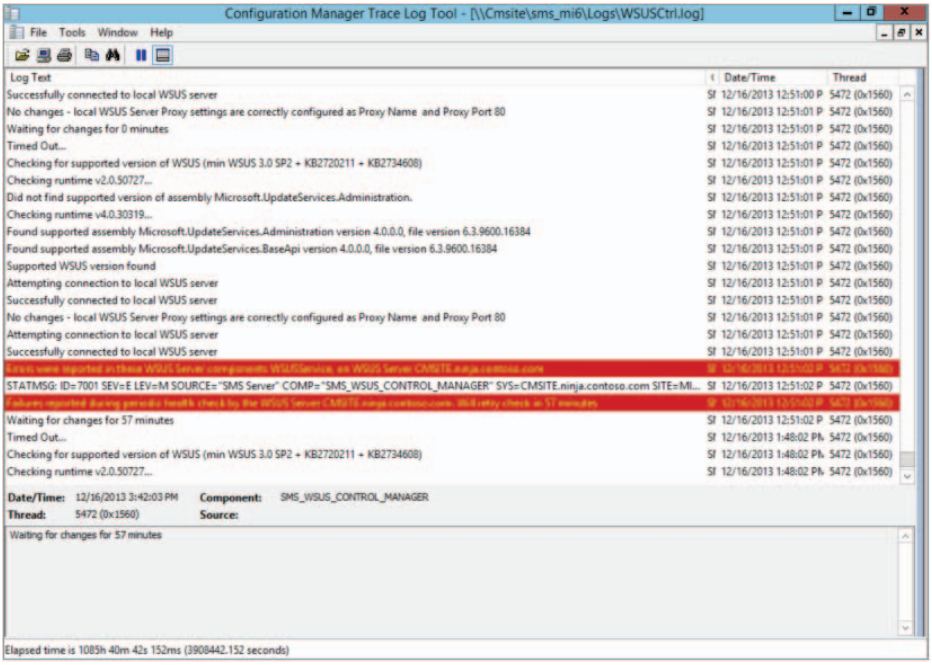


FIGURE 19.3
Highlighted error in CMTrace



The other tool you need is a reference to all the log files. We covered the log files and their locations earlier in this chapter, and this information is a great reference. So now you are well equipped to troubleshoot a ConfigMgr 2012 R2 site using the log files from the client or site systems, using the status messages in Configuration Manager, or using the web reporting feature of Configuration Manager.

Status Messages

Now that you have seen where the log files reside on both the client and servers, we will cover the troubleshooting components in the Configuration Manager 2012 R2 console. Microsoft has continued to provide status messages within the console.

Limitations of Status Messages

Status messages do have some limitations. The first limitation is that site systems must be able to communicate in order for status messages to be transferred back; if a site system component cannot report back because of a failed network connection, it might still be showing that it is available. Another limitation is that most client messages are transferred as low priority by default, and during high utilizations these messages might be delayed.

Although status messages have some limitations, they can still be vital weapons in the troubleshooting arsenal of a ConfigMgr administrator. They just shouldn't be the only source for troubleshooting, however.

Status messages reside in one location, which is why they provide some benefit when troubleshooting. They are arranged in one place so you can quickly see the health of the site at a glance. To view the site status, in the ConfigMgr console choose Monitoring ➢ Overview ➢ System Status ➢ Site Status.

The System Status dashboard is a summarized collection of the status of all the reported sites for easy viewing, and it has drill-down capability for each message. The System Status dashboard is organized into two categories, Component Status and Site Status, as shown in Figure 19.4.

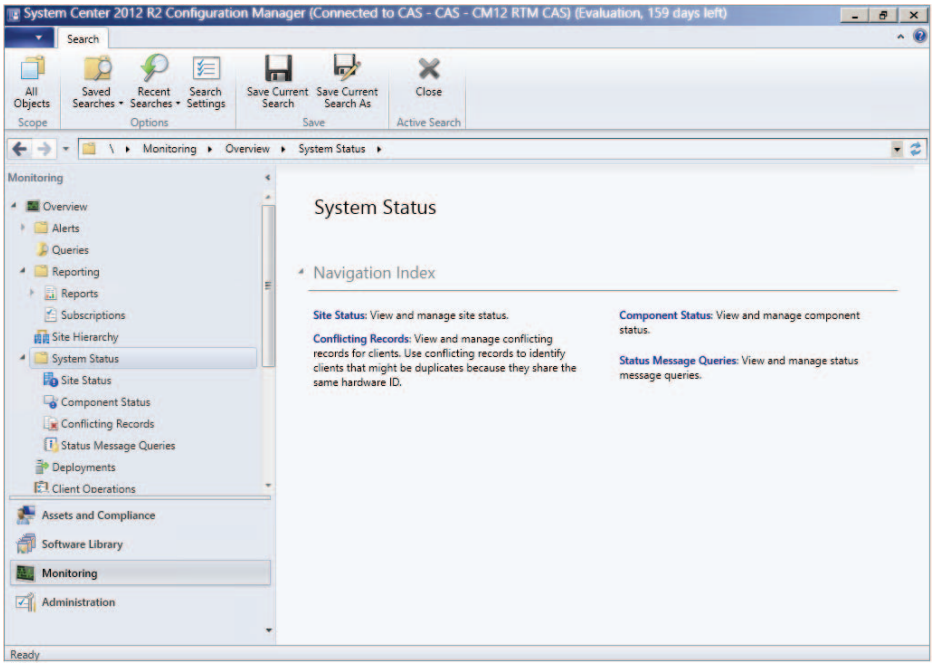


Figure 19.4
The Site Status dashboard

To dig deeper into a Component Status message to see details about a problem, follow these steps:

1. In the ConfigMgr console, choose Monitoring ➢ Overview ➢ System Status ➢ Component Status.
2. Select the component you want to investigate. In this example, we will select the component SMS_DATABASE_NOTIFICATION_MONITOR.
3. Right-click the component, and select Show Messages ➢ All, as shown in Figure 19.5.

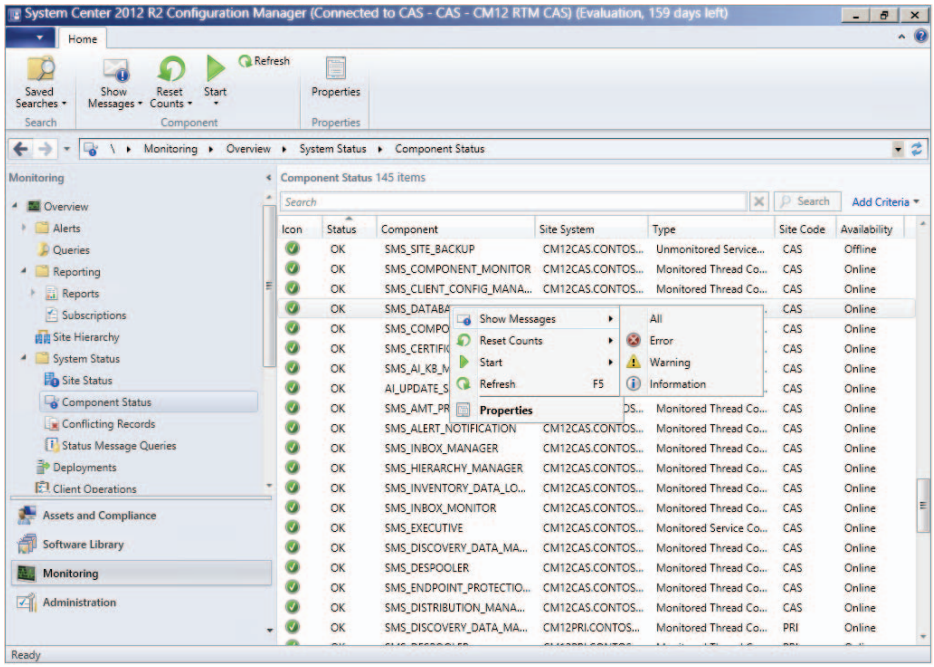


FIGURE 19.5 The Show Messages menu

This opens the Configuration Manager Status Message Viewer for *<Site Code> <Site Name>* window, as shown in Figure 19.6.

Note that you can filter the returned messages by selecting All, Info, Warning, or Error messages.

4. Within the Configuration Manager Status Message Viewer window, double-click any of the messages to get a detailed view of the message, as shown in Figure 19.7.

FIGURE 19.6
The Configuration Manager Status Message Viewer window

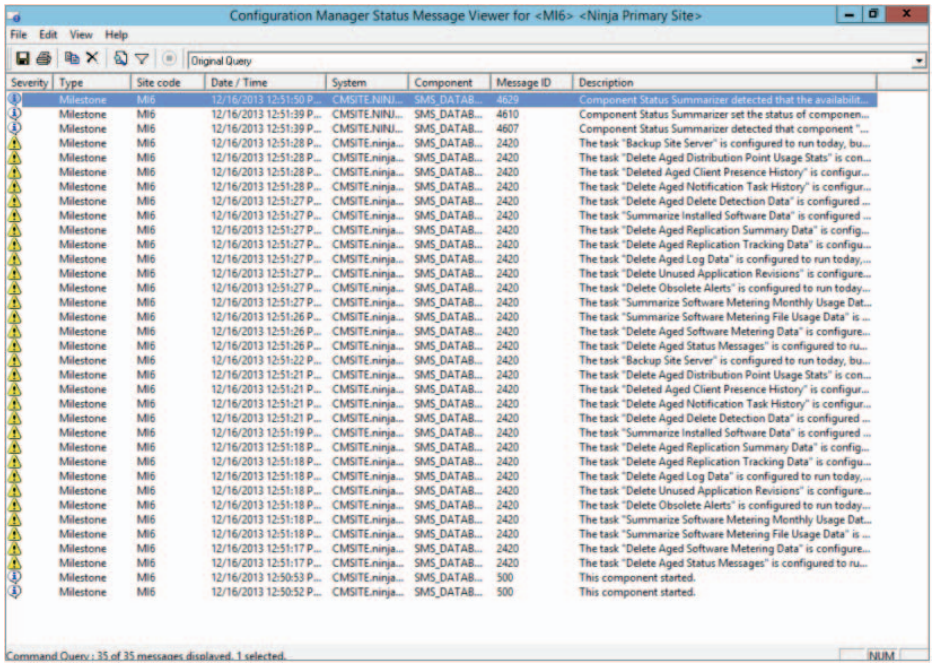
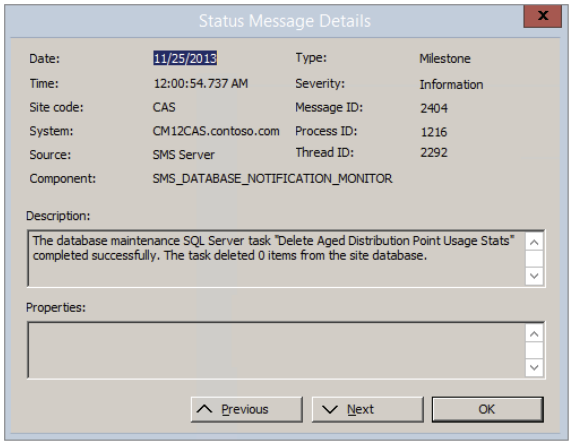


FIGURE 19.7
The Status Message Details dialog box



USING WEB REPORTS TO VIEW STATUS MESSAGES

You can view status messages from the Web Reports tool within Configuration Manager 2012 R2. This is beneficial in case you are not able to access the ConfigMgr console or you have limited access to it. In either case, you can browse to your reporting point web console and view the status messages within a browser.

As discussed in Chapter 13, "Reporting," web reports allow administrators to provide focused views of a ConfigMgr site database via a web browser and can be set up within a

dashboard to give managers an at-a-glance overview of the hierarchy. Table 19.7 lists the reports available in the Status Messages category.

Table 19.7: Status Messages reports

Name	Description
All Messages for a Specific Message ID	Lists the messages with a single message ID
Clients Reporting Errors in the Last 12 Hours for a Specific Site	Lists the computers and components reporting errors in the last 12 hours and the number of errors reported
Component Messages for the Last 12 Hours	Lists the component messages for the last 12 hours for a specific site code, computer, and component
Component Messages for the Last Hour (for a Specific Site)	Lists the status messages created in the last hour by a specified component on a specified computer in a specified SMS site
Count Component Messages for the Last Hour for a Specific Site	Displays the number of status messages by component and severity reported in the last hour at a single specified site
Count Errors in the Last 12 Hours	Displays the number of server component error status messages in the last 12 hours
Fatal Errors (by Component)	Lists the computers reporting fatal errors by component
Fatal Errors (by Computer Name)	Lists the computers reporting fatal errors by computer name
Last 1000 Messages for a Specific Computer (Errors and Warnings)	Summarizes the last 1,000 error and warning component status messages for a single specified computer
Last 1000 Messages for a Specific Computer (Errors)	Summarizes the last 1,000 error server component status messages for a single specified computer
Last 1000 Messages for a Specific Computer (Errors, Warnings, and Information)	Summarizes the last 1,000 error, warning, and informational component status messages for a single specified computer
Last 1000 Messages for a Specific Server Component	Summarizes the most recent 1,000 status messages for a single specified server component

As you can see, Microsoft has provided some nice reports out of the box for status messages. Of course, you can create your own report or modify any of the existing reports to fit your needs.

Deployment Status

Configuration Manager offers deployment status via the Monitoring workspace in the ConfigMgr console; you can monitor the deployment of all software (software updates, compliance settings, applications, task sequences, packages, and programs). To view this section of the console, do the following.

1. In the Configuration Manager console, choose the Monitoring workspace.
2. In Overview, choose Deployments.
3. To review general status information about an application deployment, select a deployment, and then choose the Summary tab of the Selected Deployment window.
4. To review deployment details for a compliance state and the devices in that state, select a deployment, and then, at the bottom of the screen in the Compliance Statistics section, click View Status.
5. To review information about the application's deployment type, select a deployment, and then click the Deployment Types tab of the Selected Deployment window.

Applications in Configuration Manager support state-based monitoring, which allows you to track the last application deployment state for users and devices. These state messages display information about individual devices. As you can see in Table 19.8, you can review the different states within the deployment.

TABLE 19.8: Application deployment state

COLUMN NAME	DESCRIPTION
Success	The application deployment succeeded.
In Progress	The application deployment is in progress.
Unknown	The state of the application deployment could not be determined.
Requirements Not Met	The application was not deployed because it was not compliant with a dependency or a requirement rule.
Error	The application failed to deploy because of an error.

You can view additional information for each compliance state, which includes subcategories within the compliance state and the number of users and devices in this category. For example, the Error compliance state contains three subcategories:

- Error Evaluating Policy
- Content Related Errors
- Installation Errors

When more than one compliance state applies for an application deployment to a user who has more than one device, you will see the aggregate state that represents the lowest compliance. For example, if a user logs into two devices, and the application is successfully installed on one device but fails to install on the second device, the aggregate deployment state of the application for that user is Error.

Use these subcategories to help you to quickly identify any important issues with an application deployment. You can also view additional information about which devices fall into a particular subcategory of a compliance state.

Distribution Status

The Configuration Manager console provides improved content monitoring, including the status for all package types in relation to the associated distribution points, including the content validation status for the content in the package, the status of content assigned to a specific distribution point group, the state of content assigned to a distribution point, and the status of optional features for each distribution point.

The console provides a Content Status node in the Monitoring workspace (see Table 19.9). Inside this workspace you can review the information of the different packages and how many distribution points have been targeted. This is very similar to the old package status on Configuration Manager 2007. To monitor the content status and view the status, follow these steps:

1. In the Configuration Manager console, choose Monitoring.
2. In the Monitoring workspace, under Overview, expand Distribution Status, and then choose Content Status. The packages are displayed.
3. Select the package for which you want detailed status information.
4. At the bottom of the screen, in the Completion Statistics area, click View Status. Detailed status information for the package is displayed.

Table 19.9: Content status monitoring

Column Name	Description
Software	Displays the name of the package
Type	Displays the type of content
Source Version	Displays the version number of the source files
Date Created	Displays the time and date the package was last changed
Targeted	Displays the total number of distribution points that have a copy of this package
Installed	Displays the total number of distribution points that have a copy of the current version
Pending	Displays the total number of distribution points that have had a failure in copying the package but have not exceeded the number of retries allowed and are currently retrying to copy the package or are in the state of removing the old package
Failed	Displays the total number of distribution points that have exceeded the number of retries and were unsuccessful at copying the package
Size	Displays the size of the package source folder
Source Site	Displays the site code of the site where the content was created
Package ID	Displays the package ID

Distribution Point Group Status

This view can be found in the Monitoring workspace in the Configuration Manager console; here you can review information such as the distribution point group name, description, how many distribution points are members of the distribution point group, how many packages have been assigned to the group, distribution point group status, and compliance rate. You can also identify errors for the distribution point group, how many distributions are in progress, and how many have been successfully distributed. To perform this action, take the following steps:

1. In the Configuration Manager console, choose Monitoring.
2. In the Monitoring workspace, under the Overview, expand Distribution Status, and then choose Distribution Point Group Status. The distribution point groups are displayed.
3. Select the distribution point group for which you want detailed status information.
4. In the bottom section, in the Distribution Statistics area, click View Status.

   Detailed status information for the distribution point group is displayed.

Distribution Point Configuration Status

On this node you can review what attributes are enabled for the distribution point, such as PXE, multicast, and content validation, as well as the distribution status for the distribution point. To view this information, perform the following steps.

1. In the Configuration Manager console, choose Monitoring.
2. In the Monitoring workspace, under the Overview, expand Distribution Status, and then choose Distribution Point Configuration Status. The distribution points are displayed.
3. Select the distribution point for which you want distribution point status information.
4. In the results pane, click the Details tab.

   Status information for the distribution point is displayed.

System Status

The System Status home page will highlight all the site systems within your Configuration Manager infrastructure and show a summary of the systems. Table 19.10 displays the information shown when you browse to the System Status home page by choosing the Monitoring workspace ➢ Overview ➢ System Status in the Configuration Manager console.

Table 19.10: System status

Column Name	Description
Status	Displays the status of the ConfigMgr 2012 site and any child site. The status will be OK, Warning, or Critical.
Site System	Displays the NetBIOS name of the site system.
Site System Role	Displays the role assigned to the site system.

Column Name	Description
Storage Object	Displays the name and location of the storage unit.
Total	Displays the total available disk space.
Free	Displays the total available free space.
Free Disk (%)	Displays the percentage of available free space.
Down Since (Time)	Displays the time when the site system could not be contacted.
Availability	Displays whether the site system is currently online or offline.

Because of the comparatively slower replication speed of status messages, most ConfigMgr administrators will focus on the log files of the client, the server, and often a combination of both. Because there are so many log files, to keep track of which log file contains the information needed for troubleshooting every ConfigMgr administrator needs two tools:

CMTrace With this tool you can view the log file in real time.

Flowcharts These usually explain how each process works and its flow.

Troubleshooting Configuration Manager Deployment

If you experience issues deploying ConfigMgr 2012, you should first look into the following areas to see whether the issue is related to permissions, disk space, network connectivity, or timing:

Permissions Permissions are extremely important to ConfigMgr deployment. If ConfigMgr does not have appropriate rights to make the connection, then the operation will fail. Admins using the ConfigMgr console will need the appropriate permissions for WMI, for DCOM, for NTFS, and within ConfigMgr itself.

Disk Space Disk space is used to store the site database, packages, software updates, inventory, and collected files; all of these can use up a lot of disk space. How much space is used depends on your environment, but you should always verify that you have sufficient disk space to store all the data within Configuration Manager.

Network Connectivity Network connectivity is a key requirement of Configuration Manager. The site system must be able to communicate with other site systems and clients. As stated earlier, sometimes the network connectivity might be down but the status messages have not updated, so you need to ensure the clients and servers can connect to each other.

Timing Patience is not always a trait of ConfigMgr administrators, but it is an important one to develop. Some tasks within Configuration Manager, Active Directory, and Windows in general take some time to complete. That is why examining the log files is so important.

Troubleshooting Configuration Manager Database Replication

Database Replication in Configuration Manager 2012 R2 (shown in Figure 19.8) is based on the Data Replication Service (DRS). This depends on two SQL features: SQL Server Service Broker and Change Tracking; these have nothing to do with transactional replication. This

replication is very important in ConfigMgr, and for this reason you need to ensure that this replication is working at all times. SQL Server Service Broker manages internal and external processes that can send and receive guaranteed async messages by using a data manipulation language. Messages can be sent to a queue in the same database as the sender, to another database in the same SQL instance, or to another SQL instance on a remote server. To better understand this concept you can visit the following site: `http://technet.microsoft.com/en-us/library/gg712701.aspx#database_replication`.

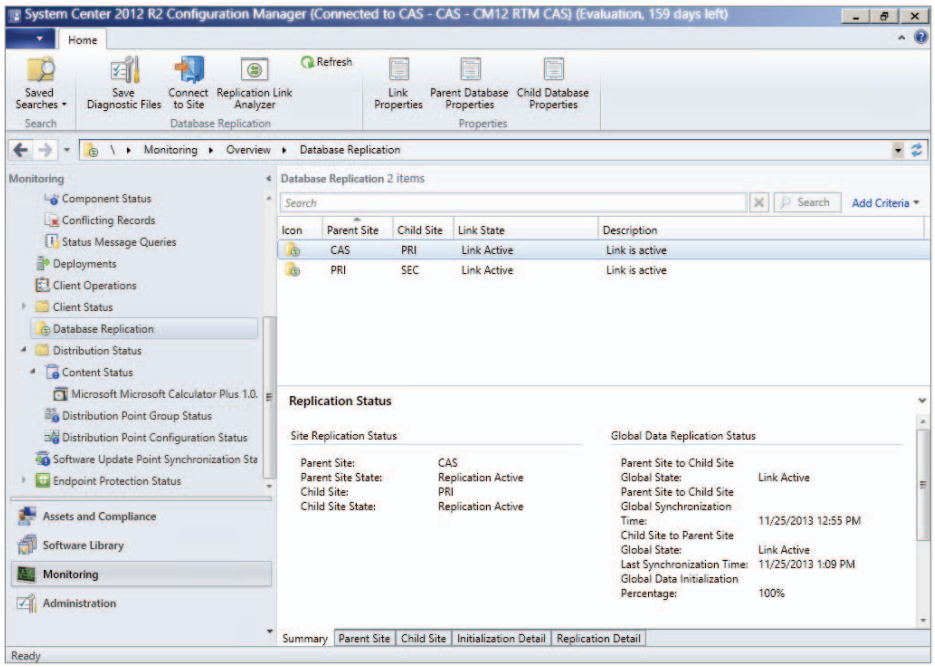


FIGURE 19.8 The Database Replication node

To look at the status of the current database replication, choose the Monitoring workspace ➢ Overview ➢ Database Replication.

A SQL communication link is a logical entity that is used to reflect the overall status of SQL communication between two sites. The link reflects the overall status of global and site data being replicated between two sites.

Each global and site data replication link will have one of the following states:

Link Active This state implies that data is being replicated as per schedule.

Link Failed This state implies that data is not being replicated because of errors. This state can also be caused when communication does not occur for more than 25 minutes.

Link Degraded This state implies that no communication has occurred for approximately 15 minutes. Regular replication intervals are approximately every 2 minutes, so a 15-minute delay in communication could indicate a degraded link.

Link Error This state implies that the replication data has synced but with errors; these errors could be due to failed data validation or conflicts.

Data Types

There are various data types in Configuration Manager. Objects that will be replicated in Configuration Manager are based on these types.

The type of data generated at the Central Administration Site and primary sites and replicated across the hierarchy is called *global data*. Since this data is globally available, it can be modified or deleted from the Central Administration Site or any primary site, regardless of where it was created, provided proper Role-Based Access Control (RBAC) permissions are configured.

The following elements are part of global data:

- Collections
- Packages
- Programs
- Deployments
- Configuration items
- Software updates
- Task sequences
- OS images (boot images, driver packages, and the like)
- Site control file
- System resource list (site servers)
- Site security objects (roles, scopes, and so on)
- Client authentication
- Client discovery

Global data replication is built on the Service Broker infrastructure provided by SQL Server.

Primary sites generate *site data*; it is potentially replicated to the Central Administration Site but never replicated between primary sites. You can view this process in Figure 19.9. Since this data is visible only at the Central Administration Site and the primary site where the data originated, it cannot be modified or deleted from other primary sites. If the data needs to be modified, it can be modified only at the originating site.

The following elements are part of site data:

- Collection membership
- Alerts
- Hardware inventory
- Software inventory and metering
- Status messages
- General site data
- Asset Intelligence CAL track data

- Software distribution status details
- Software updates replicated site data
- Software updates non-replicated site data
- Status summary data
- Component and site status summarizers
- Client health data
- Client health history
- Wake On LAN
- Quarantine client restriction history

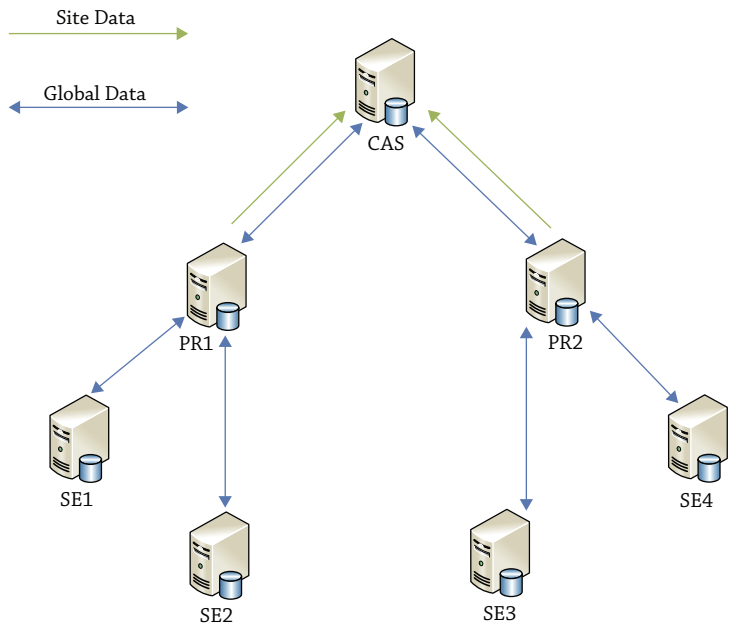


FIGURE 19.9
Replication flow

DRS Initialization

The process of DRS initialization is as follows:

1. A receiving site sends an `init` request to the sending site for the required replication group.
2. The sending site uses `bcp` (Bulk Copy Program) to export all the data from the tables in the replication group. During this phase, you can open the `RCMCtrl.log` file, as shown in Figure 19.10.
3. Hierarchy replication copies the BCP files and sends a count of each row for each table to the receiving site inbox via the senders. To view the details about this process, see Figure 19.11.

FIGURE 19.10
RCMCtrl .log viewed in CMTrace.exe

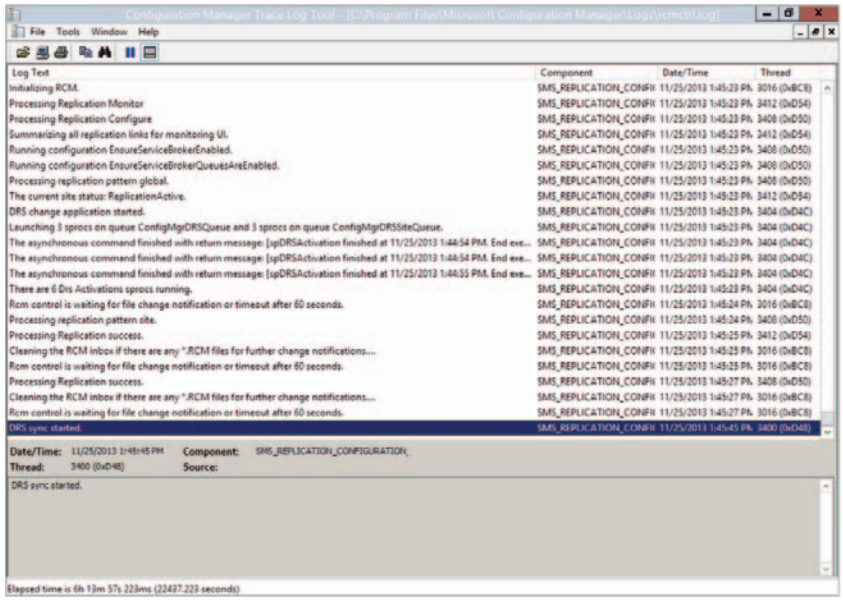
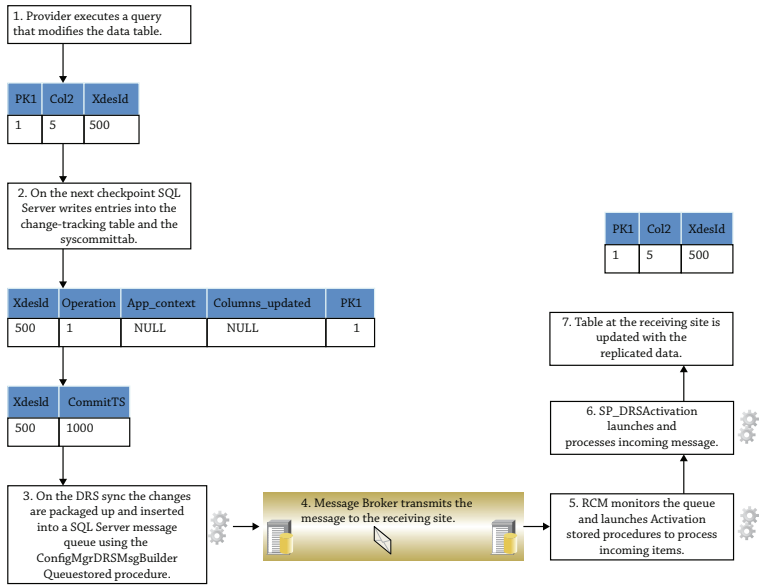


FIGURE 19.11
Replication process



By default ConfigMgr starts with the Replication Configuration Data group, which contains the data about other groups to be replicated.

To evaluate this process you can then open the `RCMCtrl.log` at the primary site or CAS (Figure 19.10).

You can also open SQL Server Management Studio and expand the Configuration Manager database ➢ Programmability and locate the `spDiagDRS` stored procedure. Executing this stored procedure will show the different statuses of the data types and the link status between sites.



Real World Scenario

Troubleshooting Contoso

In this scenario you have been asked to go onsite to troubleshoot a problem with a Contoso hierarchy. Contoso is a financial institution that has a Tier 3 Configuration Manager hierarchy. As an engineer, you will review Contoso's environment for potential issues.

The Situation

The hierarchy is not replicating changes to a specific package.

Troubleshooting Steps

The first thing you have to do is understand Contoso's issues and goals. It's important to follow a process to resolve the problem. I always use the following process—seven steps of problem solving:

1. Define and identify the problem.
2. Analyze the situation.
3. Identify possible solutions.
4. Select the best solution.
5. Evaluate the solution.
6. Develop an action plan.
7. Implement the solution.

If you follow these steps, you will be able to resolve most Configuration Manager issues or any problems that may arise.

1. Define and identify the problem.

   One package is not replicating to a primary site.

2. Analyze the situation.

   Find this package on the Configuration Manager 2012 R2 console and note the Package ID. Then validate the current state of the database replication. In the Monitoring workspace you can validate the content by using Content Monitoring.

   At this point you know the Package ID, the distribution points this package is currently deployed to, and the potential issues this package may have. But the problem is still not fixed because you have only identified potential issues.

3. Identify possible solutions.

   During the review of database replication you found out that the current state is Link Degraded. In this chapter you learned that this state indicates that SQL has not been able to communicate with the server in the past 15 minutes. To continue troubleshooting this issue you must open `RCMCtrl.log` using `CMTrace.exe` and find out the last time the package was replicated to this site. If the replication hasn't occurred in the past 15 minutes, you must try to resolve other potential issues related to communication.

4. Select the best solution.

   You have determined that the issue identified in step 3 is related to communication with the primary site. You contact the network administrator and explain the communication problems you are having on the site. The administrator promises to resolve the issue within a couple of hours. To solve the problem you decide you will reinitiate database replication, resend the package to the primary site, and review the log files for confirmation that the package has replicated.

5. Evaluate the solution.

   The solution provided in step 4 was to reinitiate database replication. You also need to review the replication process as described in Figure 19.11. If this solution is the one that makes the most sense to implement in this environment, then it is the one you will execute. It's very important to evaluate the solution in detail before implementing it.

6. Develop an action plan.

   To be able to accomplish this, you need to understand what you must do to solve this problem:

   - You need to determine what people need to be involved and what tasks they need to perform.
   - Since the solution provided is related to communication, you must explain your action plan to the network administrator, who will evaluate the communication.
   - You will execute a new database replication on the Configuration Manager 2012 R2 environment; it's a good idea to have the database administrator involved just in case you need to back out your plan or have them help you understand the process involved in resolving the situation.
   - Once all the tasks are outlined and everyone understands what is needed to solve the problem on the site, you can execute the plan on the environment.

   You should always have a back-out plan just in case your solution doesn't solve the problem. If that happens, you'll need to go back to step 1.

7. Implement the solution.

   Now that you have all the tasks figured out, go ahead and execute the plan to solve this problem:

   a. Get the database replication in place again.
   b. Resend the package to the distribution point.
   c. Evaluate the log files to confirm the package was sent out to the distribution point.
   d. Validate that the content is on the primary site where you were having the problem.

   After executing each task, the problem on the primary site should be solved and the package should be replicated. If the problem is still not fixed at this point, go back to steps 5 and 6, and make sure you understand the situation correctly.

Solving a problem can take from minutes to hours in a Configuration Manager environment; it will depend on the complexity of the hierarchy you are working on and the type of problem. This was a quick guide to resolving issues in a structured way. Always make sure you understand the problem correctly before attempting to solve it.

Understanding these processes is key to troubleshooting DRS replication in Configuration Manager. Be sure to review this process and learn how the DRS and stored procedures are executed in this process for a successful replication.

Additional Tools

One other set of tools available to you for troubleshooting is the System Center 2012 R2 Configuration Manager Toolkit, available at `www.microsoft.com/en-us/download/details.aspx?id=36213`. This toolkit contains 15 tools to help you manage and troubleshoot ConfigMgr 2012 R2. We cover the tools next, divided into server-based tools and client-based tools.

Server-Based Tools

DP Job Manager (DPJobManager) helps you troubleshoot and manage ongoing content distribution jobs to ConfigMgr distribution points, as shown in Figure 19.12.

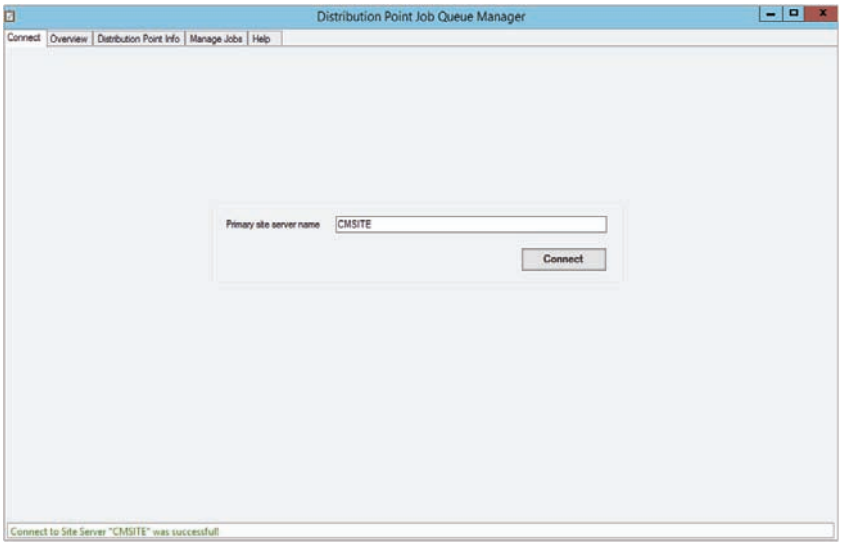


FIGURE 19.12 DP Job Queue Manager

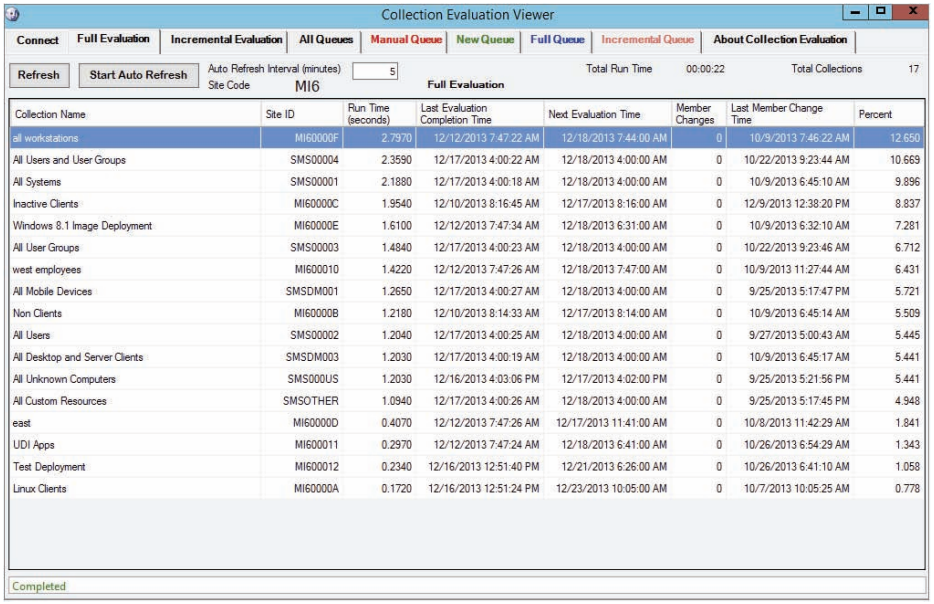
With DP Job Manager open, you enter the name of the primary site server where those distribution points are connected. You can then choose the Overview, Distribution Point Info, Manage Jobs, or Help tabs to get additional details about the queues.

Collection Evaluation Viewer (CEViewer) assists you in troubleshooting collection evaluation–related issues by viewing collection evaluation details, as shown in Figure 19.13.

Once you're connected to the primary site, you will be able to review the current collections. For example, as you can see in Figure 19.13, from the current collections that are performing a full evaluation in this list, you can determine the collection name, site id, run time, last evaluation time, next evaluation time, member changes, last member change time, and percent of members. All this information is useful when troubleshooting collections. Besides the full evaluation, there are other tabs that will help on this troubleshooting. Here are more details about each tab.

- Incremental Evaluation will show you all the collections that have been marked with the Use Incremental Updates For This Collection.
- All Queues gives you a dashboard of what is currently running on all the queues.
- Manual Queue is for collections that have been manually selected for evaluation from the administrative console UI.
- New Queue is for newly created collections.
- Full Queue is for collections due for full evaluation.
- Incremental Queue is for collections with incremental evaluation.

FIGURE 19.13 Collection Evaluation Viewer



This is a very good tool that will help you address the question of why a collection has not updated.

Content Library Explorer assists you in troubleshooting issues with and viewing the contents of the content library, as shown in Figure 19.14.

Once you open Content Library Explorer, it will ask you to connect to the distribution point by entering its FQDN. Once you're connected to the distribution point, you will be able to browse the content library and select the package ID you are trying to troubleshoot.

You can use the Security Configuration Wizard Template for System Center 2012 R2 ConfigMgr to help secure the site server. The wizard is an attack-surface reduction tool for the Microsoft Windows Server 2008 R2 operating system. Security Configuration Wizard determines the minimum functionality required for a server's role or roles and disables the functionality that is not required. An example of this is shown in Figure 19.15. With this file you can then use the Security Configuration Wizard (SCW) to apply the .xml file to the site server by running the following command line: `scwcmd register /kbname:ConfigMgr /kbfile:c:\program files (x86)\ConfigMgr 2012 toolkit\ServerTools\ConfigMgr2012SCW.xml`

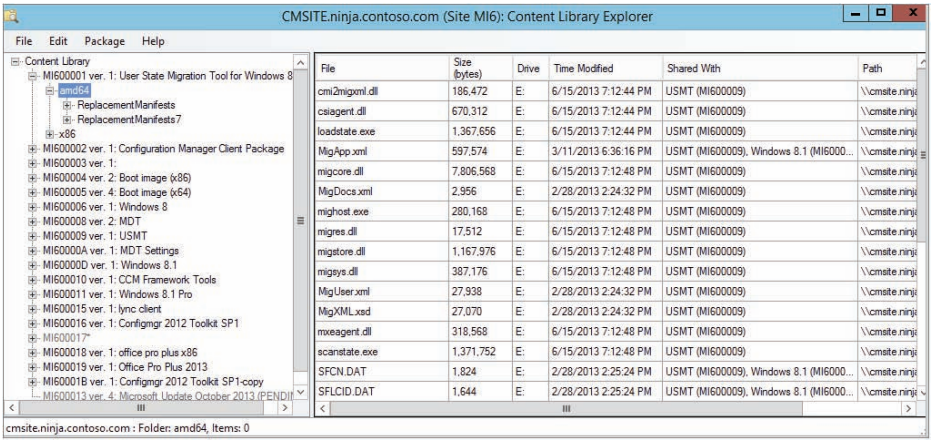


FIGURE 19.14 Content Library Explorer

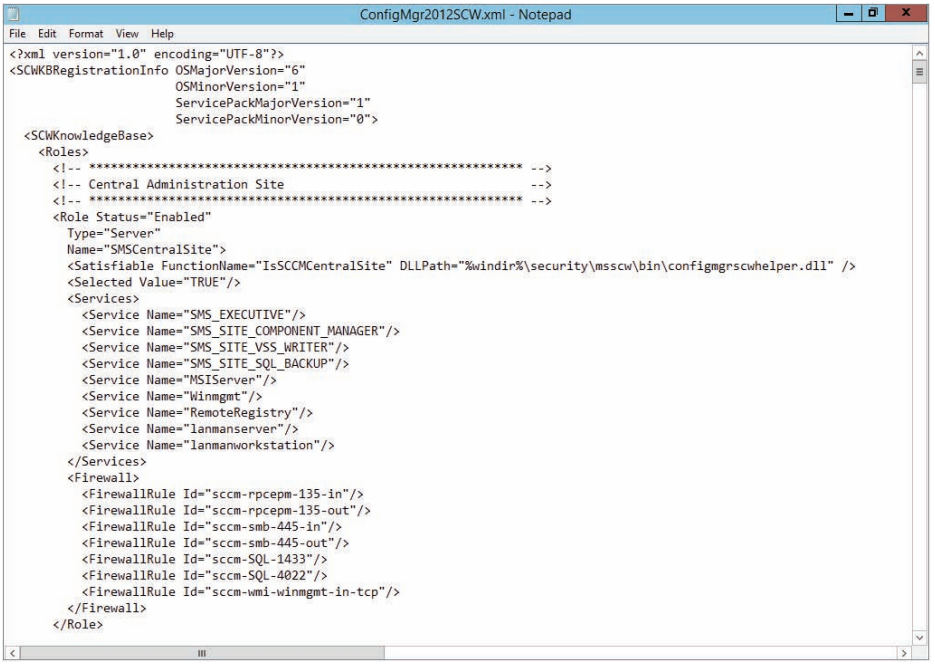
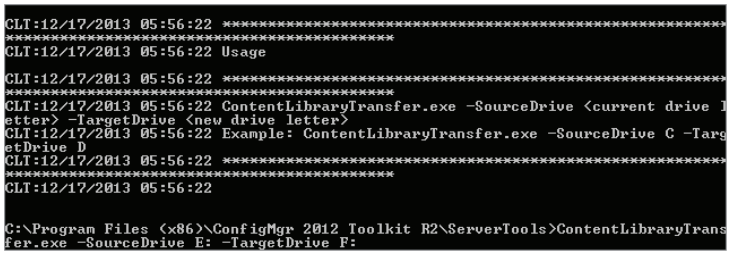


FIGURE 19.15 Security Configuration Wizard Template XML file

Content Library Transfer is a tool that transfers content from one disk drive to another, as you can see in Figure 19.16.

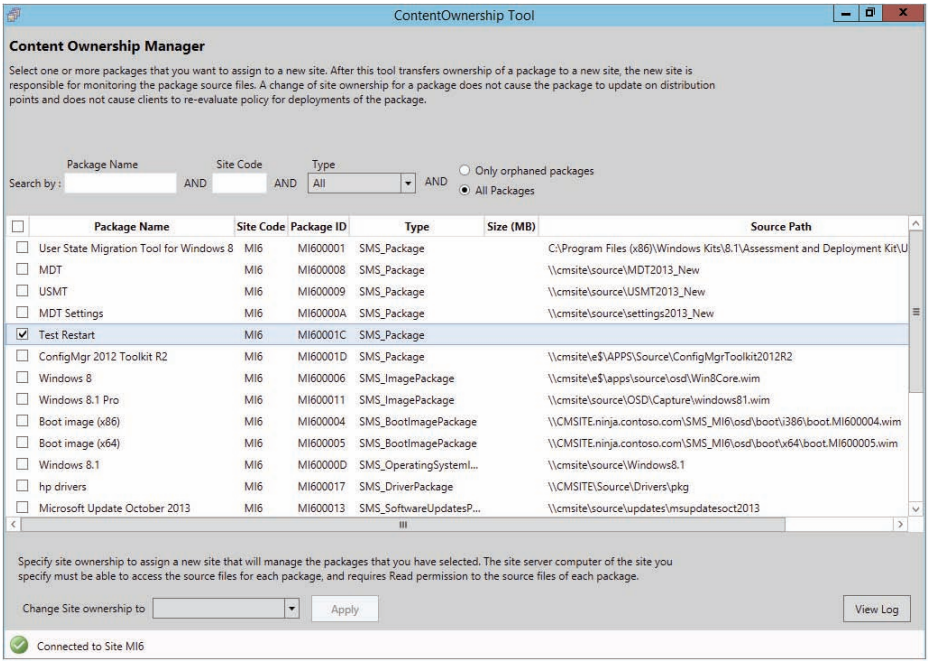
You can imagine a distribution point whose drive is filling up quickly, and you need to move the content from one drive to another but don't want to rebuild the distribution point. Instead, you can move the content from one drive to another by entering the following command: `ContentLibraryTransfer.exe -SourceDrive X: -TargetDrive Y`. Once the command finishes, the content library will be located on the new drive.

FIGURE 19.16
Content Library Transfer



The Content Ownership Tool changes the ownership of orphaned packages (packages without an owner site server), as shown in Figure 19.17.

FIGURE 19.17
Content Ownership Tool



If you select Only Orphaned Packages, all orphaned packages will be displayed in the list. You can also choose All Packages to see all the package names. Once you find an orphaned package, you can click Change Site Ownership To and specify the new site; then click Apply.

The Role-Based Administration Modeling and Auditing Tool (RBA Viewer) helps administrators model and audit RBA configurations, as shown in Figure 19.18.

RBA Viewer is a great tool to use to model the security role; more importantly, you can audit a user by clicking the green play button at the top of the screen. Then all you need to do is enter the user information and click Check. This will display the current assignments and console view.

The Run Metering Summarization Tool (runmetersumm) runs the metering summarization task to analyze raw metering data, as shown in Figure 19.19.

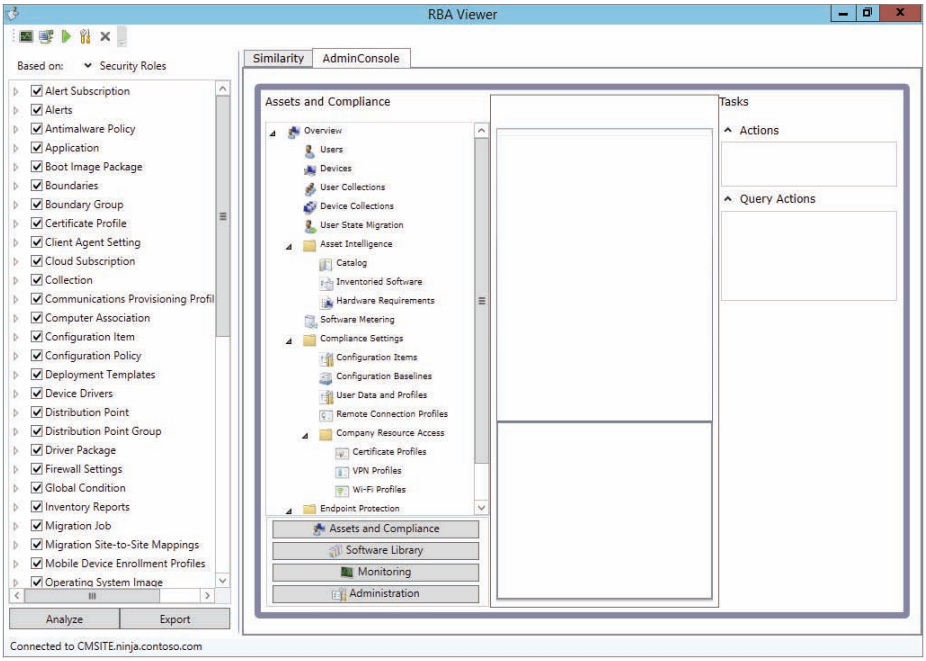


FIGURE 19.18
RBA Viewer

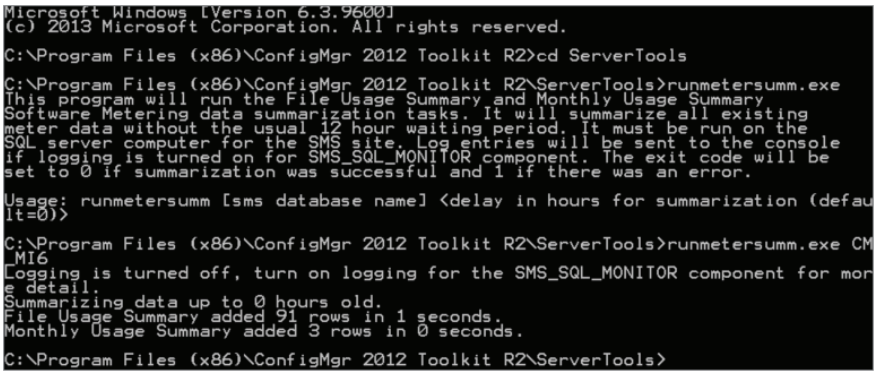


FIGURE 19.19
Run Metering Summarization Tool

You can use this tool to update the software metering data. This needs to run at the primary site server where the data is going to be inserted. Once that's completed, you will be able to run the software metering reports with no problem.

Client-Based Tools

Client Troubleshooting Tool (CliSpy) is a tool that helps you troubleshoot issues related to software distribution, inventory, and software metering on ConfigMgr clients, as shown in Figure 19.20.

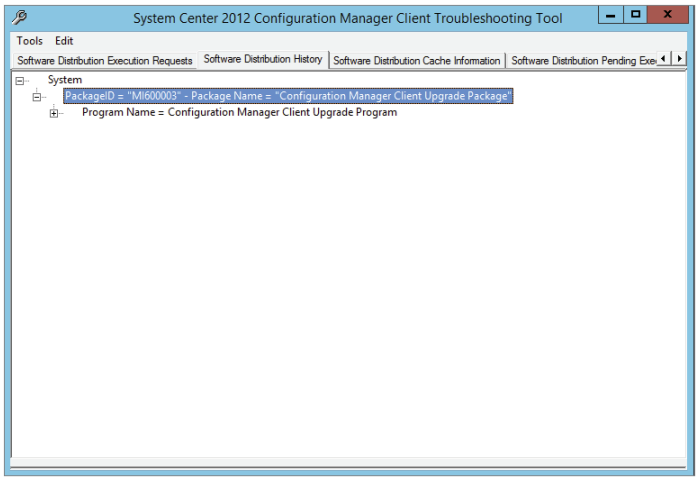


FIGURE 19.20
Client Troubleshooting Tool (CliSpy)

To use this tool, you must click Tools and connect to the client you are currently troubleshooting. Once you're connected, you will have the option to review each tab and identify the potential problem on the client.

Configuration Manager Trace Log Viewer is a tool used to view log files created by ConfigMgr components and agents. This tool was covered earlier in this chapter and is shown in Figure 19.3; it is the day-to-day tool of every ConfigMgr administrator.

The Deployment Monitoring Tool is a graphical user interface designed to help troubleshoot applications, updates, and baseline deployments on ConfigMgr clients, as shown in Figure 19.21.

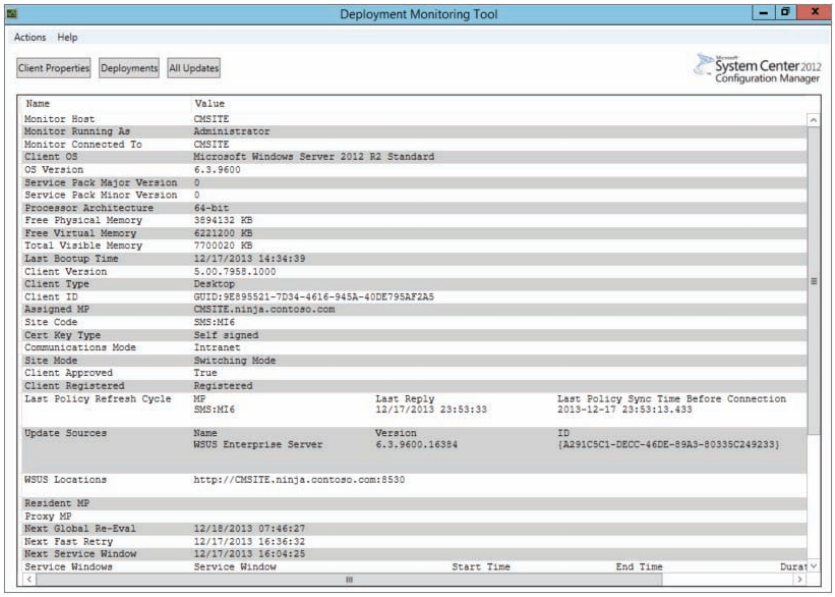


FIGURE 19.21
Deployment Monitoring Tool

Once open, it will connect by default to the current computer. To connect to another computer, you must click Actions and then click Connect To Remote Machine. Once you have chosen the computer to troubleshoot, you can click Client Properties to review the information of the client. You can click Deployments to validate what deployments have been completed on the machine or are optional to the machine. This will also include baselines deployments, as mentioned earlier. You can also click All Updates; this status will display all the current installed or missing.

Policy Spy is a policy viewer that helps you review and troubleshoot the policy system on ConfigMgr clients, as shown in Figure 19.22.

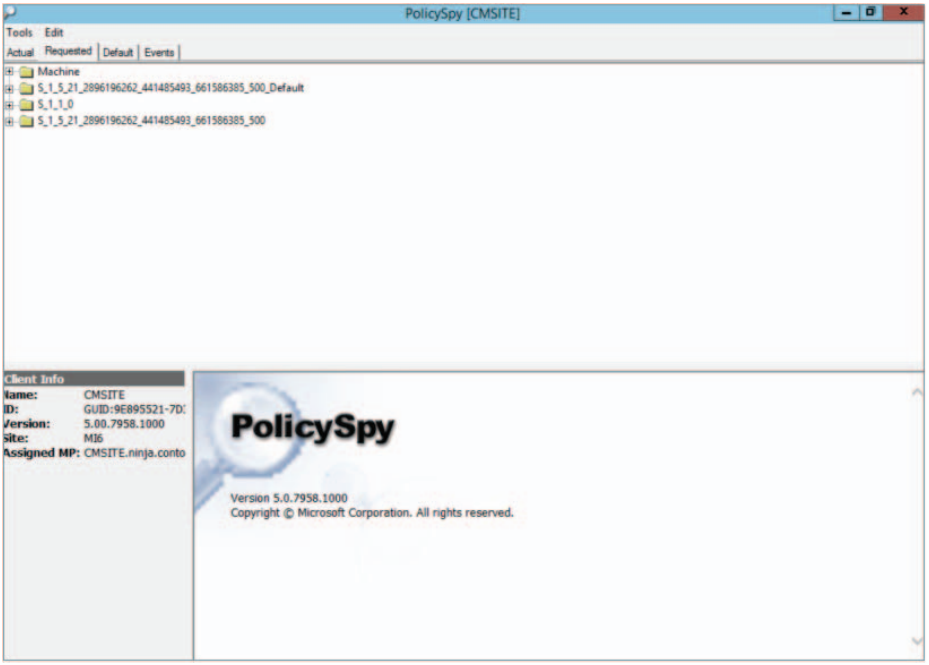


FIGURE 19.22
Policy Spy

You can use the Power Viewer Tool to view the status of the power-management feature on ConfigMgr clients, as shown in Figure 19.23.

The Send Schedule Tool is used to trigger a schedule on a client or trigger the evaluation of a specified DCM baseline. You can trigger a schedule either locally or remotely, as shown in Figure 19.24.

FIGURE 19.23
Power Viewer

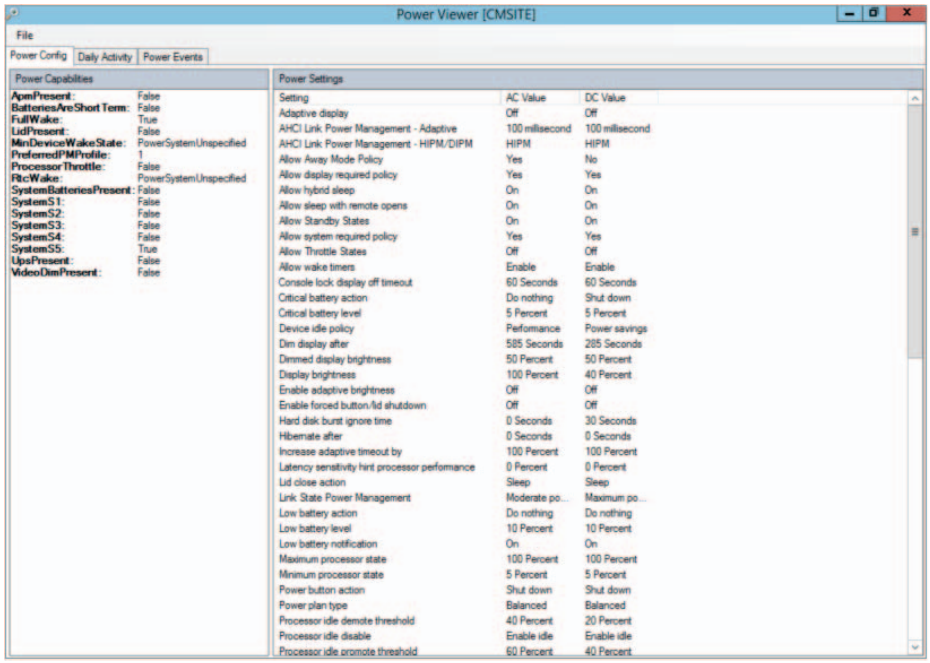
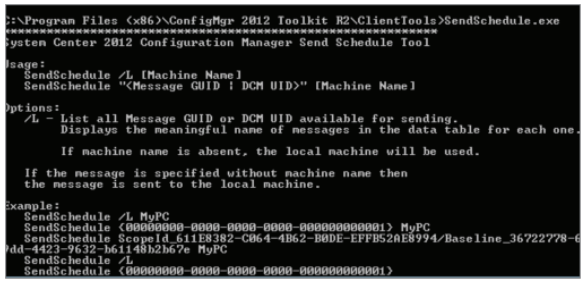
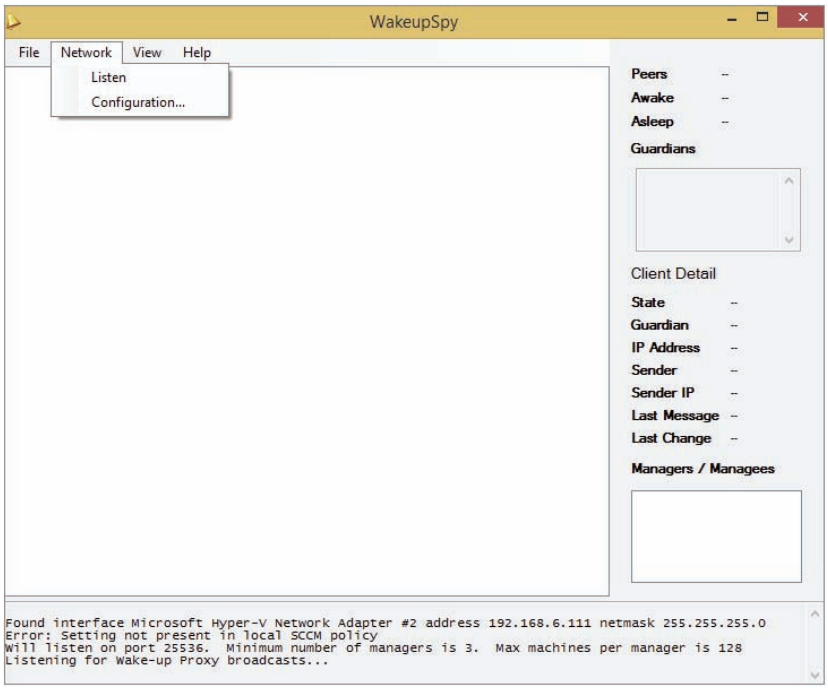


FIGURE 19.24
Send Schedule Tool



Wakeup Spy is a tool that provides a view of the power state of ConfigMgr client computers, as shown in Figure 19.25.

FIGURE 19.25
Wakeup Spy



The Bottom Line

Create a basic maintenance plan. Setting up a basic maintenance plan is a vital step to ensure the proper health of your Configuration Manager 2012 R2 hierarchy.

Master It How do you create a basic maintenance plan?

View log files using CMTrace. Although using CMTrace is not a requirement for viewing log files, it is highly recommended because CMTrace constantly monitors the opened file for updates.

Master It Use CMTrace to view log files.

Troubleshoot DRS replication. To view the current status of the ConfigMgr DRS replication and to know the latest information about the changes being requested on the site, it's important to be familiar with the log file and the replication process.

Master It To view the latest changes on the replication process, what log file do you need to open to view this information?

Master the troubleshooting steps. It's important to outline the steps to identify a problem and solve it.

Master It How many steps were needed to troubleshoot Contoso?



Appendix

The Bottom Line

Each of The Bottom Line sections in the chapters suggest exercises to deepen skills and understanding. Sometimes there is only one possible solution, but often you are encouraged to use your skills and creativity to create something that builds on what you know and lets you explore one of many possible solutions.

Chapter 2: Planning a Configuration Manager Infrastructure

Plan and design a Central Administration Site. One of the first questions you will ask yourself while starting to design and plan a new Configuration Manager 2012 hierarchy is "Do I need a Central Administration Site?" The answer to this question is essential for your final design.

Master It Determine when a CAS is needed.

Solution When there is a need for more than one primary site in your Configuration Manager infrastructure, you also need a CAS. Adding a CAS to the Configuration Manager 2012 hierarchy is not possible, so be sure to plan your Configuration Manager 2012 hierarchy correctly.

Plan and design an effective Configuration Manager 2012 infrastructure. When planning and designing a new Configuration Manager 2012 infrastructure, it is important to plan your site placement appropriately. The design rules for primary sites have changed from how they were in Configuration Manager 2007.

Master It Understand the reasons for *not* needing an additional primary site implementation.

Solution You don't need to implement an additional primary site for the following reasons:

- Decentralized administration
- Logical data segmentation
- Discrete client settings
- Languages
- Content routing for deep hierarchies

Identify the enhancements to the distribution point site system role. Distribution points in older versions were used to provide local points for accessing content and later also for App-V streaming. In Configuration Manager 2012 distribution points do a lot more.

Master It Distribution points have been enhanced. What roles and components are merged with the new distribution point, and what's new?

Solution Tricky question; not only are the PXE-enabled distribution points and the multicast-enabled distribution points merged with the new distribution point, but also the old branch distribution point and the distribution share are merged. The distribution point can be installed on Windows versions for servers and computers. Some new features of the distribution point are

- Bandwidth control
- Scheduling and throttling data synchronization
- Ability to specify drives for content
- Content validation on the distribution point
- Support for content prestaging

Prepare your current Configuration Manager 2007 environment for migration to Configuration Manager 2012. An in-place upgrade of Configuration Manager 2007 to Configuration Manager 2012 is not supported. Configuration Manager 2012 has a migration feature within the feature set to enable side-by-side migration.

Master It How can you as a Configuration Manager administrator or consultant prepare a current Configuration Manager 2007 environment for migration to Configuration Manager 2012?

Solution Steps you can take to prepare for the migration to Configuration Manager 2012 include the following:

- Flatten your hierarchy where possible.
- Plan for Windows Server 2008 R2, SQL 2008, and 64-bit.
- Start with the implementation of BranchCache with Configuration Manager 2007.
- Move from web reporting to SQL Reporting Services.
- Avoid mixing user and device-collection definitions.
- Use the UNC path in your packages instead of local paths.

Chapter 3: Migrating to Configuration Manager 2012

Determine what you are able to migrate with the migration feature. The new migration feature in Configuration Manager 2012 allows you to migrate the old Configuration Manager investments to Configuration Manager 2012 side by side. In earlier versions you were able to migrate the server in place or side by side by replicating data, but no real manageable migration feature was available.

Master It With the migration feature you cannot migrate things like the following:

- Queries
- Security rights for the site and objects
- Configuration Manager reports from SQL Server Reporting Services
- Configuration Manager 2007 web reports
- Client inventory and history data
- AMT client-provisioning information
- Files in the client cache

To keep it positive, identify what objects you are able to migrate with the migration feature of Configuration Manager 2012.

Solution Almost every investment you made in Configuration Manager, whether Configuration Manager 2007 or 2012, you are able to migrate to a new Configuration Manager 2012 environment. The following list includes all the objects that can be migrated:

- Collections
- Advertisements and deployments
- Boundaries
- Boundary groups (Configuration Manager 2012 only)
- Global conditions (Configuration Manager 2012 only)
- Software distribution packages
- Applications (Configuration Manager 2012 only)
- Virtual application packages (Configuration Manager 2007 only)
- App-V virtual environments (Configuration Manager 2012 only)
- Software updates
  - Deployments
  - Deployment packages
  - Deployment templates
  - Software update lists
  - Software update groups (Configuration Manager 2012 only)
  - Automatic deployment rules (Configuration Manager 2012 only)

- Operating system deployment
  - Boot images
  - Driver packages
  - Drivers
  - Images
  - Installer
  - Task sequences
- Settings management
  - Configuration baselines
  - Configuration items
- Asset intelligence
  - Catalog
  - Hardware requirements
  - User-defined categorization list
- Software metering rules
- Saved searches (Configuration Manager 2012 only)

Discover which migration approach is supported. Configuration Manager 2012 provides migration features that can be used for your migration of Configuration Manager 2007 to Configuration Manager 2012.

> **Master It** With the earlier upgrades or migrations of Configuration Manager in your mind, what migration approaches are supported when migrating from Configuration Manager 2007 to Configuration Manager 2012?
>
> **Solution** Configuration Manager 2012 officially supports only one migration approach, the side-by-side migration approach, when using the migration feature. The wipe-and-load approach is used only if you do not need to migrate anything from your old Configuration Manager 2007 environment.

Ascertain what kind of interoperability is supported during the migration. Interoperability like that supported in earlier versions is no longer supported; nevertheless, the migration feature of Configuration Manager 2012 supports some kinds of interoperability during the migration process. Depending on the size of your Configuration Manager 2007 or Configuration Manager 2012 source hierarchy, the migration can take some time.

> **Master It** Interoperability like you were used to in SMS 2003 and Configuration Manager 2007 is no longer supported. Give two examples of interoperability features in Configuration Manager 2012.
>
> **Solution** For interoperability purposes you are able to use shared distribution points in the process of migrating objects from a source Configuration Manager hierarchy to the

new Configuration Manager 2012 hierarchy. Another interoperability feature is the ability to re-migrate update objects. In other words, you can re-migrate objects that have been updated in the source Configuration Manager hierarchy while migrating other objects.

Migrate packages and programs to the new application model. The classic packages just migrated to Configuration Manager 2012 can be used and targeted to collections of users and computers, but Configuration Manager is built around a new application model that allows you to implement user-centricity in your Configuration Manager 2012 environment.

Master It Converting classic packages to the application model is not a feature of Configuration Manager, but with extra software it can be done from the Configuration Manager 2012 console in a couple of different ways. What is the name of the tool that you use to convert the classic packages, and what are the steps to convert a classic package?

Solution The tool that is used for converting classic packages is Package Conversion Manager. Package Conversion Manager fully integrates with the Configuration Manager 2012 console.

The steps you need to take to convert a classic package are as follows:

1. Analyze the classic packages for their readiness state.
2. Convert classic packages that have a readiness state of Automatic.
3. Fix and convert the packages that have a Manual readiness state.
4. Test the applications before deploying them.

Chapter 4: Installation and Site Role Configuration

Understand Configuration Manager 2012 R2 sites and the new approach to hierarchy design. Configuration Manager 2012 R2 has three types of sites: the Central Administration Site, which is new, and the primary and secondary sites, which are familiar. Although two of the three site types are familiar, their use and approach to hierarchy design—or whether a hierarchy is needed at all—are quite different now.

Master It Describe the purpose of each site type and map each to specific management needs.

Solution

- Central Administration Site: Only present if a hierarchy is being configured. Provides centralized administration for the hierarchy but no direct client management.
- Primary site: Clients are assigned to primary sites, and this is where they receive management instruction, regardless of where in the hierarchy the client might be located.
- Secondary site: This type of site is of use only in situations where bandwidth conditions are so slow or unstable as to require a site server to throttle even small traffic, such as discovery and inventory information.

Construct a Configuration Manager 2012 R2 hierarchy. The site hierarchy in Configuration Manager 2012 R2 consists of the site types just described. The approach to design is very different from the previous version, with the number of primary sites being limited to a single tier. The chapter walked through configuring a hierarchy with all three site types.

Master It Describe a Configuration Manager 2012 R2 site hierarchy. Detail components needed for site-to-site communication and security settings.

Solution

- Hierarchies always consist of a CAS and at least one primary child site. Additional primary child sites might be in place as well. Secondary sites should rarely be used but may be added if needed.
- Site-to-site communication requires site servers to have proper addresses and senders to be configured and correct credentials to be assigned where applicable.
- ConfigMgr 2012 installations create several local security groups that are used to grant access to site resources and facilitate site-to-site communication.

Determine when to expand a hierarchy and when to simply add a site system role for additional service. A major design goal of Configuration Manager 2012 R2 is simplified hierarchy design. Administrators familiar with previous versions of Configuration Manager may be tempted to retain old hierarchy approaches when designing Configuration Manager 2012 R2. Taking such an approach will often lead to inefficient designs and additional server cost and in some cases simply won't work.

Master It Understand the changes in sites and site components that lend themselves to hierarchy simplification and enable parity management with fewer site servers.

Solution

- Distribution point modifications include the ability to throttle content directly to remote distribution points. In addition, it is now possible to install distribution points on workstation systems directly where needed.
- Boundary groups simplify hierarchy configurations by allowing administrators to strictly define which distribution points are used to service specific client content requests.
- The updated security model in Configuration Manager 2012 R2 allows administrators to scale out a single site while still maintaining logical separation of user role and function. There is no longer a technical need to have separate primary sites for servers and workstations. When managed properly, a single primary site is able to manage both seamlessly while protecting resources from access by unauthorized users.

Deploy and configure the various site system roles available per site. There are many roles available to enable management at a site. Understanding each role and the service it delivers is critical to getting the most out of an investment in Configuration Manager 2012 R2.

Master It Review critical system roles and understand the services that are enabled through each.

Solution

- Critical site system roles are those that are required for basic ConfigMgr functionality at most sites. These include the management point and distribution point roles.

- Management points facilitate client-to-site server communication.
- Distribution points store content that may be needed by clients of the site.

Chapter 5: Cloud Integration

Test cloud distribution points before going into production. Before you go into production with cloud-based distribution points, you should test the service to make sure it meets your needs. The tools required for testing and the trial service are free.

Master It Creating a cloud distribution point is easy, but there are prerequisites that need to be met. You will need a Windows Azure account and Visual Studio to create the management certificate.

Solution Test cloud distribution points at no cost to you before you go into production. Get a free trial Windows Azure subscription that will allow you to test the service. You can also download for free Visual Studio Express 2013 to create the management certificate.

Control cloud distribution points usage costs. Don't set and forget your cloud-based distribution points. Monitor its usage so you can control your costs. Monitoring usage will also help you determine when it is time to scale up.

Master It Make sure you have control of the charges associated with data transfers from your Windows Azure subscription.

Solution Take advantage of Configuration Manager alerts and options to control the amount of data you copy to cloud distribution points. Be proactive in monitoring the amount of data requested by your clients. Also be smart about what you copy to your cloud distribution points. Does it make sense to have large applications like Microsoft Office on your cloud distribution points? Probably not.

Simplify your hierarchy. Since the early development stages of Configuration Manager 2012, Microsoft has been telling us to flatten or simplify our Configuration Manager hierarchies. Cloud-based distribution points provide you with another opportunity to do so.

Master It Flatten your Configuration Manager hierarchy. There are probably site roles that could be decommissioned by deploying cloud-based distribution points.

Solution Consider replacing secondary sites or distribution points on remote locations and using cloud-based distribution points instead. When decommissioning a role is not possible, consider extending your private cloud hierarchy to the cloud. Don't forget the flexibility and scalability cloud-based distribution points bring to Configuration Manager.

Chapter 6: Client Installation

Configure boundaries and boundary groups. Before starting any client installation, verify that you have configured a boundary group for site assignment.

Master It Let Configuration Manager Forest Discovery automatically create the boundaries and add them to the correct boundary groups.

Solution Once you have configured Forest Discovery, add the automatically created IP subnets to a new or existing discovery group.

Select the relevant discovery methods. You configure discovery methods in the Configuration Manager console. The Active Directory discovery methods all require a schedule and an LDAP path. There are schedules for delta and full discovery. In Configuration Manager 2012, delta discovery will also find changes to existing objects; this eliminates the need to run a full discovery more than once a week.

Master It Always know what you want to discover and where. Based on that knowledge, configure the needed discovery methods.

Solution The correct discovery method depends on how you want to deploy clients and work with features like application deployment. For a client push installation to work, it is a good idea to configure Active Directory Computer Discovery. On the other hand, if you want to deploy applications to end users, you also need to configure Active Directory User Discovery.

Employ the correct client installation methods. When configuring the client installation methods, make sure you know the pros and cons for each method. Some require firewall settings; others require local administrative permissions. You need to make sure that all the required settings are in place. Do not start any installation until you have the needed site systems, boundary groups, and command lines specified.

Master It Configure the correct command-line properties and ensure they will work for all environments (local forest, workgroup, and DMZ). Create multiple client push installation accounts, and ensure that you have a good understanding of the three phases (pre-installation, installation, and post-installation).

Solution Configure the command-line properties in the properties for the client push installation method. That way you ensure that the properties are always replicated to Active Directory and can be read during the client installation.

Furthermore, you should add the command-line properties that will also work in another forest and workgroup in the client push properties.

Manage Unix/Linux and Mac devices. Configuration Manager 2012 provides support for managing Unix/Linux and Mac computers as devices. You are now able to manage your entire computer infrastructure from a single management console.

Master It Understand the installation methods available for deploying the Configuration Manager client to the Unix/Linux computers and Mac computers. Remember that client push cannot be used for these devices.

Solution The client installation process for Unix/Linux devices has several required parameters, such as the site code, the management point, and the installation package to use. Use the optional parameters to define other client configuration features, such as the fallback status point to utilize or the folder that will be used for the client installation.

Ensure client health. Client status might not be the first task you think about when implementing a system like Configuration Manager. But it is crucial to the daily administration that you can trust the numbers you see in the reports and in the console. One way to ensure that is by making certain that all clients are healthy and are providing the server with up-to-date status messages and discovery information.

Master It Discuss the different environments that exist in your organization, and use that information when configuring client health alerts. Make sure that you know the client activity during a normal period and that you have a set of defined SLAs for each of the environments (laptops, road warriors, servers, call center, and so on).

Solution Create unique collections corresponding to each computer role type that you have. In the properties for every collection, configure the unique client status values.

Chapter 7: Client Health

Detail client health evaluations in Configuration Manager 2012. Health evaluations and remediations take place daily on every Configuration Manager 2012 client in the hierarchy. This information is updated at the site and is available for review on every client and also summarized for every client across the hierarchy.

Master It List the health evaluations and remediations that take place on Configuration Manager clients.

Solution

- Review the `CCMEval.log` file to see all evaluations and remediations that are taking place on clients.
- Review the `CCMEval.xml` file to understand the details behind each evaluation.

Review client health results in the Configuration Manager console. Client health data is available in several locations of the console to allow access to health for individual devices and summarized data for all clients in the hierarchy.

Master It List the locations in the console where individual client health and summarized client health data are accessible.

Solution

- Individual client health data is available by viewing devices individually in collections.
- Summarized client health data is available in the Monitoring workspace of the Configuration Manager console by choosing the Client Status node and then the Client Activity and Client Check nodes.
- Configuration Manager 2012 R2 reports also offer a view into client health data.

Chapter 8: Application Deployment

Explain the options available for Application Deployment. The new Application Deployment model is a significant and welcome change for deploying software in the enterprise. There are many new components including a rules-based Requirements engine, the ability to detect whether the application is already installed, the option to configure application dependencies and relationships, and more.

Master It List several configuration options available for applications and deployment types.

Solution

- Applications: The ability to publish in the Application Catalog, define supersedence, and reference information.
- Deployment types: The ability to set dependency information, specify criteria defining whether an application is already installed, configure requirements, and set return codes.

Detail the various components required for Application Deployment. Success with Application Deployment requires that several other Configuration Manager 2012 components be available and properly configured. The list includes management point(s), distribution point(s), IIS, BITS, the client itself, and possibly more.

Master It List the components required for configuring an application deployment.

Solution The application and at least one deployment type and deployment content must be staged on at least one available distribution point. Clients must receive the deployment and pass any configured requirements, allowing the deployment to be initiated.

Understand the role of and manage distribution points. The role of distribution points has not changed significantly in that this is the role that makes content available to Configuration Manager 2012 devices and users. The options available for implementing the role have changed significantly with the inclusion of throttling control content flow from site server to remote distribution points, the single-instance storage approach for placing content on distribution points, the ability to detect content corruption, and the requirement that all distribution points be BITS enabled.

Master It Discuss the differences between implementing a distribution point role on the site server locally and remotely.

Solution

- Local distribution point: Content is transferred by local file copy; there is no ability to throttle a local distribution point.
- Remote distribution point: Content is transferred by network file copy without compression. The ability to throttle content is available, but content is not compressed.

Chapter 9: Software Updates

Plan to use Software Updates. You can use the same method of deployment intelligence that was used in Chapter 2 to gather information for planning to implement Software Updates. This will be very helpful in making sure that you get the most out of the Software Updates feature for your organization.

Master It What is the first step in gathering deployment intelligence when you are planning to implement Software Updates?

Solution You must determine what needs to be accomplished with Software Updates.

Configure Software Updates. Before you can utilize Software Updates in your environment, you must set up and configure the various components of this feature.

Master It What is the first thing you have to install before you can use Software Updates?

Solution You must install Windows Server Update Services (WSUS) 3.0 SP2. You can use either the full install or the WSUS administrative console, depending on what you are setting up.

Use the Software Updates feature to manage software updates. The hardest thing to do in SMS 2003 relating to patch management was to programmatically prioritize software updates that are critical so they can be deployed with a higher priority than other updates.

Master It What does Configuration Manager provide that can help with prioritizing software updates?

Solution Configuration Manager now includes the severity of all of the updates that are synchronized into the Configuration Manager database. With that data you can sort updates by that category and create search criteria and update groups based on their severity level so that you can use them as a source for your software update components.

Use automatic update deployment to deploy software updates. When you deployed software in Configuration Manager 2007, you deployed software updates through a procedure that consumed a lot of time.

Master It Configuration Manager has a new feature called Automatic Deployment Rules. What kinds of updates are suitable to deploy via the automatic deployment rules?

Solution Patch Tuesday software updates and definition files for Forefront Endpoint Protection can be deployed via the automatic deployment rules. Be sure to always test the updates to see if they have any impact on your environment.

Chapter 10: Operating System Deployment

Specify a Network Access account. The Network Access account is the account Configuration Manager will use to access the system while running WinPE.

Master It How do you specify the Network Access account?

Solution Open the Configuration Manager 2012 console, and do the following:

1. Choose the Administration workspace and expand Overview ➢ Site Configuration ➢ Sites.
2. Select one of the sites for which you want to configure the Network Access account, and click Configure Site Components on the Home tab of the ribbon.
3. Select Software Distribution.
4. Select the Network Access Account tab, set the Network Access account to the account created earlier, and click OK.

Enable PXE support. PXE support in Configuration Manager is used to begin the operating system deployment process. The PXE feature responds to Configuration Manager clients making PXE boot requests.

Master It How do you set up PXE support?

Solution Open the Configuration Manager 2012 console, and do the following:

1. Choose the Administration workspace and expand Overview ➢ Distribution Points.
2. Select the site server on which the distribution point resides, and click Properties on the Site Role area of the ribbon.
3. Select the PXE tab and click Enable PXE Service Point.

Update the driver catalog package. The driver catalog allows you to add drivers to the already created packages and images you have within your organization so you are not constantly re-creating your images when you get a new machine in your environment.

Master It How do you update the driver catalog package?

Solution From within the Configuration Manager console, do the following:

1. Choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Drivers.
2. Click Import Driver on the Home tab of the ribbon of the Configuration Manager console.
3. Browse to the network location of the drivers you want to import.
4. Specify which package and boot images you want to import the specific drivers into.

Update an image from the console. In the past it was a big issue to keep your images up to date; no easy procedure existed. In Configuration Manager 2012 a feature called Schedule Updates exists to update your Windows images.

Master It How do you update your Windows images?

Solution From within the Configuration Manager console, do the following:

1. Choose the Software Library workspace, expand Overview ➢ Operating Systems, and select Operating System Images.
2. From there select a Windows image and click Schedule Updates in the Home tab of the ribbon of the Configuration Manager console.

The process of updating the images is scheduled; after finishing, the wizard and the update will start automatically.

Chapter 11: Inventory and Software Metering

Configure and manage Software Inventory. Configuring Software Inventory has changed in Configuration Manager 2012, although the client-processing part is almost the same as in Configuration Manager 2007.

Master It By default, Configuration Manager does not inventory for any file types. Where would you go to do that?

Solution Take the following steps:

1. Navigate to the Administration workspace, under Overview select Client Settings, and open the Default Client Settings properties.
2. Select Software Inventory.
3. Click Set Types.
4. Click the New button, and configure the files or file types you want to include in the software-scanning process.

Configure and manage Hardware Inventory. Hardware Inventory provides a wealth of information on the hardware resources in your organization. That information is vital when planning for things such as updating standard business software or upgrading the standard

operating system your organization uses. If the standard hardware inventory collected is not enough for your needs, then you have many options to extend the hardware inventory to get that vital information.

Master It Where do you enable or disable data classes in Hardware Inventory?

Solution You need to open the default client agent settings or create a custom client setting. Custom client settings can only be used when you want to enable data classes that already exist in Configuration Manager. For custom classes (or to delete classes) you need to modify the default client settings.

Configure and manage Software Metering. Keeping track of software that is installed and actually being used is a large part of being able to manage software licenses effectively. By pairing Software Metering in Configuration Manager with Software Inventory, you can get detailed information on just what software is out there and who is or is not using it. This goes a long way to help keep your software licensing in compliance.

Master It How long do you have to wait, at the very least, after you configure Software Metering before you can expect to see any data returned?

Solution You must wait at least 12 hours. Software Metering Data Summarization runs daily by default and will run only against data that is at least 12 hours old. This is required for all software metering reports to produce any meaningful data.

Chapter 12: Asset Intelligence

Enable Asset Intelligence. If you installed ConfigMgr from scratch, you will find that Asset Intelligence is not enabled by default. Depending on the data that you want information on, you will have to select the ConfigMgr Asset Intelligence reporting classes and make sure that client agents are enabled.

Master It Which classes in the Asset Intelligence Edit Inventory Classes dialog do you have to enable to use Asset Intelligence?

Solution You need to enable the following classes in the Asset Intelligence Edit Inventory Classes dialog to use Asset Intelligence:

`SMS_SystemConsoleUsage`

`SMS_SystemConsoleUser`

`SMS_InstalledSoftware`

`SMS_AutoStartSoftware`

`SMS_BrowserHelperObject`

`SoftwareLicensingService`

`SoftwareLicensingProduct`

`Win32_USBDevice`

`SMS_SoftwareTag`

Configure the Asset Intelligence synchronization point. The Asset Intelligence synchronization point is used to connect to System Center Online to synchronize Asset Intelligence Catalog information and get periodic updates.

Master It What do you need to do in order to configure the Asset Intelligence synchronization point?

Solution

- You need to configure it on only the CAS or stand-alone primary site.
- You may want to obtain an optional System Center Online authentication certificate.
- If no valid certificate is issued, you can install the Asset Intelligence synchronization point without a certificate.

Import the Microsoft Volume License Statement. In ConfigMgr you can import the Microsoft Volume License Statement and the General License Statement so that the software inventory and Asset Intelligence can count the number of licenses currently in use in the environment.

Master It What file types does ConfigMgr 2012 support for the license statements?

Solution It will be a `.csv` file if the file to be imported is a General License Statement. If you are going to import a Microsoft Volume License Statement, it will be an `.xml` or `.csv` file. You can obtain this file by logging into the following website: `http://licensing.microsoft.com`. Or you can request this file from your Microsoft Technical Account Manager or Account Manager.

Chapter 13: Reporting

Install the Reporting Services point. Installing a Reporting Services site system within Configuration Manager allows not only administrators but everyone to view reports in some fashion either via different file formats or a direct link within the Report Manager Website.

Master It What is the procedure to enable Reporting with Configuration Manager?

Solution Open the Configuration Manager 2012 console, and do the following:

1. Navigate to the Administration workspace.
2. Expand Overview ➢ Site Configuration ➢ Servers And Site System Roles.
3. Right-click the server and select Add Site System Roles.

Manage reporting security. Reporting security is an integrated part of the built-in security. You provide users with access to reports by adding them to a predefined security role or by creating a custom role with permissions to run or modify reports.

Master It Add users to a built-in security role.

Solution Open the Configuration Manager 2012 console, and do the following:

1. Navigate to the Administration workspace ➢ Overview ➢ Security ➢ Administrative Users.
2. Click Add User Or Group from the ribbon.

Create and manage report subscriptions. Creating subscriptions can be very helpful in many scenarios. You can configure subscriptions from Report Manager or in the Configuration Manager console.

Master It Create an email-based subscription.

Solution Open the Configuration Manager 2012 console, and do the following:

1. Navigate to the Monitoring workspace.
2. Expand Overview ➢ Reports.
3. Select the report, and click Create Subscription from the ribbon.

Create custom reports. Creating custom reports can be helpful in many scenarios. You will quickly find that the canned reports are very useful but may be limited for all your needs.

Master It Create a custom report.

Solution Open the Configuration Manager 2012 console, and do the following:

1. Navigate to the Monitoring workspace.
2. Expand Overview ➢ Reports, and select the appropriate folder.
3. Click Create Report from the ribbon to start the process in Report Builder.

Chapter 14: Compliance Settings

Enable the client settings. Until the client settings are enabled for your Configuration Manager clients, your clients will not evaluate any of the configuration baselines. This is the first step in using Compliance Settings to validate client settings.

Master It Enable Compliance Settings for the Configuration Manager clients.

Solution In the Compliance Settings section of the client settings, set Enable Compliance Evaluation On Clients to True.

Create configuration items. Configuration items are the pieces that make up a configuration baseline. There are a number of different configuration item types in Configuration Manager, and depending on the type you choose to create, you are presented with certain options when creating your configuration item. The steps to create configuration items were covered in the first part of this chapter, and they included several examples of how to create the different types of configuration items.

Master It Create a configuration item for an application that checks a registry string value.

Solution Start the wizard from the Assets And Compliance workspace, Compliance Settings node; make sure you have Configuration Items selected, and right-click it. Choose Create Configuration Item. In the wizard, complete the following settings:

1. On the General tab, enter appropriate information for these fields:

   Name: Application name and value description

   Description: Configuration item for …

   Categories: Add categories

2. On the Settings tab, choose New Settings ⊞ Registry Key from the menu and set the following options:

   Hive: `HKEY_LOCAL_MACHINE`

   Key: `SOFTWARE\ ...`

   Is This Registry Key Associated With A 64-Bit Application: No

   Report A Noncompliance Event When This Instance Count Fails: Yes/Checked

   Instance Operator: Greater Than

   Values: 0

   Severity: Warning

3. On the Settings tab, choose New Registry from the menu.
4. On the General tab of the new registry validation, enter the following information:

   Display Name: User-friendly name

   Description: Description of what you are checking for

   Hive: `HKEY_LOCAL_MACHINE`

   Key: `SOFTWARE\ ...`

   Value Name: Registry key value name

   Is This Registry Key Associated With A 64-Bit Application: No

5. On the Compliance Rule tab of the new registry compliance, set Data Type to String.
6. Click New on the menu in the details pane and, in the Configure Settings window that appears, configure these settings:

   Name: User-friendly name

   Description: Description of the value you are going to check for

   Operator: Equals or Other operator

   Value: Value to check the registry key for

   Severity: Warning

7. Click OK to return to the Validation tab of the new registry validation and set the following:

   Is This Registry Key Associated With A 64-Bit Application: No

   Report A Noncompliance Event When This Instance Count Fails: Yes/Checked

   Instance Operator: Greater Than

   Values: 0

   Severity: Warning

8. Click OK to save your changes to the Settings tab and move on.
9. On the Detection Method tab, select the radio button Always Assume Application Is Installed.

Define a configuration baseline. This is where you take one or more of the CIs and put them into a package that the Configuration Manager client downloads and at the scheduled time validates by checking the CIs against the computer. The Configuration Manager client then reports the outcome of those checks back to Configuration Manager, where you can then run reports to see if your clients are within the specified configuration. These steps were covered in the last section of the chapter.

Master It Assemble a configuration baseline with one or more configuration items you have created.

Solution Follow these steps:

1. In the Assets And Compliance workspace, expand Compliance Settings, and then choose Configuration Baselines.
2. Right-click and choose Create Configuration Baseline.
3. Enter an appropriate name for this baseline and a description, and select or create any categories necessary.

   The Configuration Data list displays all the configuration items or configuration baselines that are included in the configuration baseline.
4. Click Add to add a new configuration item, and choose the configuration items you have created.
5. Click OK and Apply, and your baseline will be created.
6. Deploy the configuration baseline to a collection.

Chapter 15: System Center Endpoint Protection

Differentiate between FEP and SCEP. There are several differences between FEP and SCEP, including the architecture and the deployment process.

Master It Where does SCEP store its data?

Solution Remember that FEP used two databases to store data: FEP_DB and FEP_DW. SCEP uses the ConfigMgr 2012 database to store SCEP-related data.

Deploy and configure the System Center 2012 Endpoint Protection site system and client. The three main components of enabling SCEP are as follows:

- Install and configure the Endpoint Protection site system.
- Enable and configure the SCEP client.
- Configure the antimalware policies.

Master It Do you need to create a package or application to deploy the SCEP client?

Solution No. The installation media for the System Center 2012 Endpoint Protection client (`SCEPInstall.exe`) is distributed to the managed devices as part of the ConfigMgr 2012 client install media. Remember that the SCEP client won't actually be installed on managed devices until the Endpoint Protection client is enabled and configured in an assigned client settings policy. Also remember that the Endpoint Protection client cannot be enabled until the Endpoint Protection site system role is enabled.

Create and assign an SCEP policy. SCEP has two types of policy:

- Antimalware
- Windows Firewall

The antimalware policy is used to define the antimalware settings, while the Windows Firewall policy can be used to control the configuration of Windows Firewall on managed computers. Both types of Endpoint Protection policies are created and modified in the ConfigMgr 2012 console.

Master It If you modify the default client antimalware policy and also create a custom antimalware policy with different values for the settings and apply it to a collection, which settings will be applied?

Solution Changes made to the default policy will be applied to all managed computers in the environment. However, the custom policy will override any settings that are in conflict with the default policy.

Chapter 16: Mobile Device Management

Detail the differences between lite and depth management. The management options and settings available for mobile devices will vary depending on whether lite- or depth-management options are in place.

Master It List mobile device management capabilities for lite versus depth management.

Solution Lite management of devices allows for limited device inventory, settings management, and remote wipe.

Depth management of devices allows for over-the-air enrollment, full inventory, more complete settings management, software distribution, and remote (selective) wipe.

Understand how to configure mobile device management. Properly configuring mobile device management requires addressing several potential scenarios. From a Configuration Manager 2012 perspective, though, the choice is simple: lite or depth management.

Master It List the items that need to be configured for both lite and depth management.

Solution Lite management requires a properly configured ActiveSync connection between the Exchange server and managed devices and also proper configuration of the Configuration Manager 2012 Exchange ActiveSync connector.

Depth management requires proper configuration of an enterprise certification authority, Active Directory, and several different site system roles. The site system roles include the enrollment point, enrollment proxy point, device management point, and distribution point.

The second option is configuring the Windows Intune connector and using Windows Intune as a middle tier between your Configuration Manager environment and your mobile devices.

Understand the depth-management enrollment process. From the user perspective, the enrollment process for depth management is straightforward. Behind the scenes, there are a number of moving parts. Each of these components is critical to the enrollment process.

Master It List the components required to enroll depth-managed devices.

Solution

- Enrollment web proxy site system role
- Enrollment service point site system role
- Mobile device management point
- Enterprise Microsoft certification authority
- Active Directory services and/or
- Windows Intune subscription
- Windows Intune connector

Chapter 17: Role-Based Administration

Understand the role-based administration model in ConfigMgr 2012. SMS and ConfigMgr 2007 used a class and instance security model, which could be confusing at times. ConfigMgr 2012 adopts the RBAC model, thereby making the administration of security in ConfigMgr 2012 a less-daunting task.

Master It What does RBAC stand for? And what does role-based administration mean?

Solution RBAC is an acronym for Role-Based Access Control and is the security model used in many products in the System Center suite, including ConfigMgr 2012.

Role-based administration means that the ConfigMgr 2012 administrator can use a combination of security roles, security scopes, and collections to define what the ConfigMgr administrative users can view and manage. ConfigMgr 2012 R2 introduces the ability to apply role-based administration to reports as well, greatly simplifying the process of securing access to report data.

Distinguish security roles from security scopes. Security roles and security scopes are important components of the role-based security model in ConfigMgr 2012.

Master It Can you identify the key differences between a security role and a security scope?

Solution The primary difference between the two is that a security role is used to organize tasks or functions, whereas a security scope is used to define access to objects. The security role is the action (or lack thereof if trying to block access), whereas the security scope is what is acted upon (or lack thereof if trying to block access).

Understand which objects in ConfigMgr 2012 define an administrative user. The administrative user consists of the security role, the security scope, and collections. In this chapter you learned the differences between a security role and a security scope, and you know that collections can be used to control the objects that an administrative user can access.

Master It As the ConfigMgr 2012 administrator, do you need to create a custom ConfigMgr 2012 console so that the administrative user can see only what you want them to see?

Solution No. The beauty of the role-based administration model is that the user will see only what they have access to in the ConfigMgr 2012 console. You do not need to provide a modified console for them. They simply log onto the environment with their administrative user account and open the ConfigMgr 2012 console, and they will see only the objects they have access to. Objects that they do not have access to will be hidden.

Understand how to simulate permissions in the ConfigMgr 2012 console. The RBAC model in ConfigMgr 2012 greatly simplifies the process for creating administrative users and defining what objects in ConfigMgr they can access.

Master It Besides the ConfigMgr 2012 console itself, what other tool can you use to simulate ConfigMgr user security and verify that the security model will provide the desired level of access?

Solution Utilize the RBA Viewer application from the Configuration Manager 2012 Toolkit. It will allow you to easily define new security roles, simulate the access the new role will have in the ConfigMgr console, as well as provide the ability to simulate the console experience under a specific user account.

Chapter 18: Disaster Recovery

Configure backups for Configuration Manager sites. Backing up Configuration Manager sites can be automated by scheduling the Backup ConfigMgr Site Server maintenance task. When the Configuration Manager backup service (SMS_SITE_BACKUP) starts, it uses instructions in the backup control file, located at

```
[ConfigMgr Install Location]Microsoft Configuration Manager\Inboxes\smsbkup
.box\smsbkup.ctl
```

Master It Recovering a complete Configuration Manager site is only supported with site backups from what source?

Solution The backups must be created by the Backup ConfigMgr Site Server maintenance task.

Recover Configuration Manager sites. Recovery of a Configuration Manager site requires that you do not have a Configuration Manager site installed when starting the `Setup.exe` process. The recovery process will recover data from the backup files and from a reference site provided you have a multisite hierarchy.

Master It What is site recovery designed for?

Solution It is used for repairing and resynchronizing ConfigMgr data.

Archive backup snapshots to another location. The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager site system when it fails. The next time the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, because there is no other backup to restore from.

Master It What script can you use to copy backup snapshots from the site server to a new location but is not created when ConfigMgr is installed?

Solution You can use `AfterBackup.bat`.

Reinstall the site components and reset file and registry permissions to their default settings. From time to time other administrators mess around with the default permissions that are configured on the different folders and shares created by Configuration Manager.

Master It How can you restore the file and registry permissions without performing a complete restore?

Solution Run `setup.exe` from the Start menu or from the *<Configuration Manager installation directory>*`\Microsoft Configuration Manager\bin\x64` folder. Select Perform Site Maintenance Or Reset This Site and click Next. On the Site Maintenance page select Reset Site With No Configuration Changes and finish the wizard.

Chapter 19: Troubleshooting

Create a basic maintenance plan. Setting up a basic maintenance plan is a vital step to ensure the proper health of your Configuration Manager 2012 R2 hierarchy.

Master It How do you create a basic maintenance plan?

Solution Develop a plan, similar to the guidelines discussed in the section "Creating the Maintenance Plan" in Chapter 19. Review and modify the plan on a biannual basis, and update it throughout the year to ensure nothing gets overlooked and the documentation is up to date with the current design of the Configuration Manager site.

View log files using CMTrace. Although using CMTrace is not a requirement for viewing log files, it is highly recommended because CMTrace constantly monitors the opened file for updates.

Master It Use CMTrace to view log files.

Solution ConfigMgr CMTrace is located on your installation media in `SMSSETUP\Tools\cmtrace.exe`. Click File, browse to the log file you want to review, and open it.

Troubleshoot DRS replication. To view the current status of the ConfigMgr DRS replication and to know the latest information about the changes being requested on the site, it's important to be familiar with the log file and the replication process.

Master It To view the latest changes on the replication process, what log file do you need to open to view this information?

Solution Locate the `RCMCtrl.log` file and open it using CMTrace. Locate the DRS initiation and RCM changes.

Other solutions might include executing the `spDiagDRS` stored procedure to view the current replication status and details about the data that is being replicated. You can find more details about the `RCMCtrl.log` at the beginning of Chapter 19.

Master the troubleshooting steps. It's important to outline the steps to identify a problem and solve it.

Master It How many steps were needed to troubleshoot Contoso?

Solution You need the following seven steps:

1. Define and identify the problem.
2. Analyze the situation.
3. Identify possible solutions.
4. Select the best solution.
5. Evaluate the solution.
6. Develop an action plan.
7. Implement the solution.

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

accounts and Accounts page
  client push installation, 254, *255*
  Exchange Server, **707**, *707*
  Network Access, **461–462**, *462*
  software update settings, 385
actions and Actions page
  application deployment, 336
  client installation, 265
  scheduled tasks, **275**, *276*
  software updates, 392, *392*
Active Directory (AD)
  discovery methods, **51–52**, **235–237**, *236–237*
    forests, **237–238**, *238*
    groups, **240**, *241*
    heartbeat, **240–242**, *243*
    network, **242**
    scheduling, **242–243**, *243–244*
    system, **239**, *239*
    users, **240**
  management points, **180–181**
  permissions, 135
  schema, **37–38**
  site boundaries, **44–45**
  system health validator points, 185
  Windows Intune, **728–729**, *729–730*
Active Directory Container dialog box, 235, *236*
Active Directory Domain Services, 52
Active Directory Membership setting, 404, 408, 411
Active Scripting option, 749
active software update points setup, **413**
ActiveSync connections, 705, 714–715
Activity Management Technology (AMT), 17
  enrollment point, 199–203
  out-of-band service points, **191–192**, *192–193*
Add Application Catalog Website To Internet Explorer Trusted Sites Zone option, 230
Add-CMSoftwareUpdatePoint command, 410
Add Configuration Items dialog box, 640, *641*
Add Distribution Point Groups dialog box, 483
Add Distribution Points dialog box, 483
Add Driver To Boot Images page, 498, *499*
Add Driver To Packages page, 498, *498*
Add Exchange Server Wizard
  Account page, **707**, *707*
  Discovery page, **707–708**, *708*
  General page, **705–706**, *706–707*
  Settings page, **708**
    Application settings, **713**, *714*
    Email Management settings, **711–712**, *711*
    General settings, **709**, *709*
    Password settings, **709–710**, *710*
    Security settings, **712–713**, *713*
Add Game Center Friends option, 747
Add New Collection Alerts dialog box, 288, 691, *692*
Add Operating System Installer Wizard, 468–469, *469–470*
Add Partner Software Updates Catalogs page, 438, *439*
Add Roles And Features Wizard, 399
Add Site System Roles Wizard, **161–163**, *162*, 577, *577*
  Application Catalog Web Service Point, 195–197, *197–198*
  Application Catalog Web Site Point, 197, *198*
  Endpoint Protection Point role, 209–210, *209*
  fallback status points, 189–190, *190*
  management points, 179, *179–180*
  mobile device and AMT enrollment points, 200–203, *201–202*
  out-of-band management, 191–192, *192–193*
  Reporting Services, 193–194, *194*, 586–587, *587*
  SCEP, 673, *674*
  Software Update Point, 203–208, *203–208*
  state migration points, 186–189, *186–188*, 462, *463*
  system health validator, 185
Add Software Updates window, 640, *641*
Add User Account screen, 524
Add User Or Group dialog box, 601
ADForestDisc.log file, 238
AdminConsole.msi file, 101
Administration Security report, 590
AdministrationConfig-EN.MSI file, 730
administrative console
  Asset Intelligence, **18**
  reports, 593–594, *594*
  software upgrades, 366
  upgrading, 86
  WSUS, **402**
administrative folder migration, **78**
administrative users
  creating, **789–790**
  overview, **785**, *786*
Administrator Comments setting, 324
administrators
  application deployment, 325
  computer accounts as, 152
  mobile device enrollment, **721–722**, *721–722*
  software updates, 366
ADR (Automatic Deployment Rules), **364**, 370, 687–688
ADsgdis.log file, 240
ADSysDis.log file, 239

ADusrdis.log file, 240
Advanced page
  antimalware policy, 683, *683*
  System Center Updates Publisher, 437
Advanced Settings page for Wi-Fi profiles, 666, *667*
advertisement migration, **74**
AfterBackup.bat file, 802–803
Agent Extensions Manage The Deployment Of Applications And Software Updates option, 230
agents
  client
    Asset Intelligence, 564
    settings, **227–232**, *228–229*, **390–391**, *390*
  planning, **60**
AI. *See* Asset Intelligence (AI)
AIUpdateSvc.log file, 211
AIUSMSI.log file, 211
AIUSsetup.log file, 211
alerts and Alerts page
  Application Deployment, **299**
  client, **268–270**, *269*
  client health, **287–288**, *288*
  cloud distribution points, 222, *223*
  configuration baselines, **646**
  Deploy Software Updates Wizard, 432–433, *432*
  Deploy Software Wizard, **338–339**, *338*
  deployment templates, 372
  SCEP, **690–691**, *691–692*
Alerts report, 590
All... collections, 785
All Instances Of The Objects That Are Related To The Assigned Security Roles option, 786
All security scope, 778
All Software Updates node, **423**
All Systems collection, 359
Allow Clients On A Metered Internet Connection To Download Point Or Remote Distribution Point settings, 433
Allow Clients To Share Content With Other Clients On The Same Subset option, **326**, 433
Allow Clients To Use A Fallback Source Location For Content option, **326**
Allow Mobile Devices That Cannot Be Provisioned option, 709
Allow Password Recovery option, 711
Allow Signed Content from Intranet Microsoft Update Service Location option, 393
Allow Simple Password option, 711
Allow Task To Be Run On Demand option, 278
Allow This Application To Be Installed option, 320
Allow User Policy Request From Internet Clients option, 230
Allow Users To Interact With This Program option, **330**
Allowed Message Formats option, 712, 748
Allowed Period Of Time Users Can Postpone A Required Restart To Complete The Endpoint Protection Installation (hours) setting, 231
Always Send Do Not Track Header option, 751
AMT (Activity Management Technology), 17
  enrollment point, 199–203
  out-of-band service points, **191–192**, *192–193*
Android operating system
  mobile device management, 703
  Windows Intune, 734, **737–739**, *738*
answer files, **157–159**
antimalware policy, **679–685**, *680–685*
App Rating option, 752
App-V
  applications, **349**, *350*
  virtual environment migration, 75
Apple operating system
  mobile device management, 703
  support, **29**
  Windows Intune, **734**, **739**, *740*
Application Administrator Properties window, 777, *777*
Application Administrator role, 597–599, 774–775
Application Author role, 598, 775
Application Catalog
  application deployment, 340, *341*
  application information, 308
  customizing, 197
  distribution points, **295**
  primary devices, 355
  User Device Affinity, 355
Application Catalog Customizations page, 197
Application Catalog tab for sample application, 320–321, *320*
Application Catalog Web Service Point role, 46, **195–199**, *196–198*, **720**, *721*
Application Catalog Website Point role, 46, **195–199**, *196–198*, 391
Application Deployment, **291**
  Application References, **296**
  client experience, **339–342**, *340–342*
  Create Application Wizard, **311–314**, *311–313*
  dependencies, **298**
    Application References, **296**
    BITS-enabled IIS, 300
    configuring, **345**, *345*
    default client settings, **300–308**, *301–302*
    distribution points, **299–300**
    management points, **299**
  Deploy Software Wizard, **333–339**, *334–338*
  Detection Method tab, **346**
  distribution point changes, **293–296**
  elements, **308–310**, *309–310*
  flow options, **296–298**
  new features, **291–293**, *292*
  process, **310–311**, *311*
  properties, **310**, *310*
  Requirements tab, **346–347**, *349*
  Ribbon options, **314–319**, *315–318*
  sample application, **319–323**, *319–320*
  supersedence, **343–344**, *344–345*

troubleshooting, **358–361**, *359–360*
types, **296–297**, **323–333**, *324–325*, *327–329*, *331–333*, **349–355**, *350–351*, *353–354*
User Device Affinity, **355–358**, *356–358*
Application Deployment Manager role, 598, 775
application management, **14**
Application References, **296**
Application Settings window, **713**, *714*
Application Store option, 748
Application Virtualization (App-V), **18–19**
applications
configuration items, **642–643**
migration, **75**
properties, **308**, *309*
Applications Management function, **6**
Applications node, 291, *292*, 311
Applications That Depend On This Application option, 344
Applications That Supersede This Application option, 344
Apply This Software Metering Rule To The Following Clients option, 557
archive_reports.sms file, 548–549
archiving backup snapshots, **802–803**, *803*
ASC keyword, 612
Asset Intelligence (AI), **563**
catalog, **566–568**
enabling, **575–576**, *577*
functionality, **18**
home page, **569–571**, *570*
maintenance tasks, **564–565**, *565*
migrating, **78**
reports, **571–575**, 590
requirements, **563–566**
software licenses, **578–581**, *578*, *580*
synchronization points, **569**, **576–578**, *577*
validation states, **568–569**
Asset Intelligence Synchronization Point Connection Settings page, *577*
Asset Intelligence Synchronization Point role, 46, **210–211**, *211*
Asset Intelligence Synchronization Point Settings page, 577, *577*
Asset Manager role, 596–597, *597*, 775
Assets and Compliance workspace, 524, *524*
assigned security scopes and collections, **785**, *786*
assigning policies, **687**, *687*
Associate Assigned Security Roles With Specific Security Scopes And Collections option, 786
Associated Security Roles dialog box, 601
ATM Provisioning Certificate page, 192, *193*
ATM Service Point page, 191, *192*
Authentication Method page, VPN profiles, 661, *662*
Autofill option, 749
Automatic Client Upgrade tab, 271
Automatic Deployment Rules (ADR), **364**, 370, 687–688
automatic operations
client remediation, **266–267**, *267*
client upgrades, **270–271**, *270*
management point queries, **182**
operating system image captures, **477–480**, *478–480*
publishing updates, 442
Automatic package conversion state, 105
Automatic Synchronization While Roaming option, 756
Automatic VPN page
mobile devices, 766, *767*
profiles, 663, *664*
Automatically Configure Used Device Affinity From Usage Data option, 502
Automatically Detect This Information About This Application option, 312
Automatically Distribute Content For Dependencies option, 335
Automatically Download Content When Packages Are Assigned To Distribution Points option, 425
Automatically Remove Previously Installed Antimalware Software Before Endpoint Protection Client Is Installed option, 231
Available Software Updates dialog box, 379
awebsctrl.log file, 199
awebsvcMSI file, 198

B

Background Intelligent Transfer Service (BITS)
Application Deployment, 300
client settings, 230, 300, *301*
Computer Client Agent, 391
distribution points, 165, 177
Background Intelligent Transfer setting, 230
Backup ConfigMgr Site Server task, **797–798**, **801**
archiving backup snapshots, **802–803**
configuring, **805–806**, *806*
considerations, **801–802**
copying backups, **802**
log files, **804**
Backup Site Server Properties dialog box, 828, *828*
Backup Site Server task, 805, *806*
backups, **801**
central site, **801–802**
considerations, **801–802**
copying to other locations, **802**
excluded items, **798–800**
log files, **804**
restoring, **807–810**, *809*
site servers, **805–806**, *806*
snapshots, **802–803**, *803*
troubleshooting, **807**
bank software, 567
bare metal operating system deployment, 452, **492–497**, *492*, *494*
baseline configuration, 631
clients, **643–644**, *643*
initial, **639–640**
options, **644**
rules, **640–644**, *641*, *645*
BIDS (Business Intelligence Development Studio), 585, **616–618**

BitLocker
task sequences, **507–508**, *508*
Windows To Go, 505
BITS (Background Intelligent Transfer Service)
Application Deployment, 300
client settings, 230, 300, *301*
Computer Client Agent, 391
distribution points, 165, 177
/BITSPriority property, **248–249**
Block The Following Applications In ROM option, 713
Bluetooth option, 754
Boot Image page, 476, *477*
boot images
customized, 77
legacy, **522–523**
Microsoft Deployment Toolkit, **512–513**, *512*
operating system deployment, **453–454**, *453*
packages, **466–467**
for PXE, **467–468**, *467*
task sequences, 476, *477*
bootable media
non-task sequences, **116–119**, *117*
task sequences, 459
boundaries
client installation, **244–246**, *245–246*
distribution points, **308**
migrating, **74–75**
sites, **44–45**
Boundary Groups page
distribution points, 172–173
secondary site servers, 145
state migration points, 188–189, *188*
branch office migration. *See* P2V Migration Toolkit
BranchCache feature, **43–44**
Browser option, 713
Browser page, 748–749, *750*
Build And Capture A Reference Operating System Image task sequence, 457
build-and-capture task sequence, **460**
Build And Capture Task Sequence Wizard, 468
build phase in migration, 82
Business Intelligence Development Studio (BIDS), 585, **616–618**
business IT alignment, **11**

C

caches
BranchCache feature, **43–44**
reports, 607
calcplus.msi file, 631
Calculator Plus utility, 628–629
Calendar Synchronization option, 748
Camera option, 754
Capacity Management process, **8**
capacity planning, 47
capture images
adding, **482–483**
automatic building and capturing, **477–480**, *478–480*
creating, **471–476**, *472–477*
distributing and deploying, **483**
reference computers, **480–481**, *481–482*
task sequences, 458
capture media, 459
catalogs
application. *See* Application Catalog
Asset Intelligence, **566–568**
categories
applications, 319
configuration items, **629**
Categorize option, 319
CCM registry key, 148–149, *149*
CCMAdmins property, 250
CCMAllowSilentReboot property, 250
CCMALWAYSINF property, 249
CCMCERTISSUERS property, 249
CCMCERTSEL property, 249
CCMCERTSTORE property, 249
ccmclean.exe utility, 100
CCMDebugLogging property, 250
CCMEnableLogging property, 250
CCMEval.exe file, 279
ccmeval.log file, 262, 279–280, *282*, 283
ccmeval process, 266, **279–283**, *279*, *282*
ccmeval.xml file, 262, 279, *282*, 283
CCMEval.xsd file, 279
CCMEVALHOUR property, 251
CCMEVALINTERVAL property, 251
CCMEvalReports.xml file, 279–280
CcmEvalTask.log file, 267
CCMFIRSTCERT property, 249
CCMHOSTNAME property, 249
CCMHTTPPort property, 251
CCMHTTPSPort property, 251
CCMInstallDir property, 250
CCMLogLevel property, 250
CCMLogMaxHistory property, 250
CCMLogMaxSize property, 250
CcmNotificationAgent.log file, 695
CCMrepair task, 283
ccmsetup-ccmeval.log file, 262
ccmsetup.exe utility
manual installation, **252–253**
properties, **247–252**
central administration sites (CAS), **123**
checklist, **126–127**
implementing, **127–136**, *129–135*
recovering, **811–817**, *812–816*
roles, **38–39**
software update points setup, **403–407**, *404–406*
Central Computer and Telecommunications Agency (CCTA), 2
centralized power management, **19**
.cer files, 215
Certificate Enrollment Wizard, 220–221, *221*
Certificate Export Wizard, 217–219, *217–218*
Certificate Properties page, 764, *764*
Certificate Registration Point role, 46
Certificate Template Name option, 764
Certificate Type option, 764
Certificate Validity Period option, 765
certificates
Mac client installation, 262–263
management, **215**
creating, **216–218**, *216–217*
exporting, **216–219**, *217–218*
uploading, **222**, *222*

profiles, **656–660**, *657–660*
service, **219–221**, *219–221*
Certificates page, 758–759, *758*
Certificates To Install On Mobile Devices option, 759
certmgr.log file, 772
-certpw property, 261
CEViewer (Collection Evaluation Viewer), **852–853**, *853*
change and configuration management, **12**
Change Management process, **7**
Check Application Title with Inventory Information task, 564
child sites
recovering, 817
software update points setup, **407–408**, *409*
Choose Mapping page, 502, *502*
Choose Target Collection page, 493, 516
ciagent.log file, 646
Classic Software Distribution, 292
classifications and Classifications page
Add Site System Roles Wizard, 207, *207*
software updates
classes, **386**
configuring, 415, *415*
metadata, 369
-clean property, 261
Clean Up Migration Data dialog box, 102, *102*
cleaning up migration data, **102**, *102*
Client Activity Detail tab, 283, *284*
client agents
Asset Intelligence, 564
settings, **227–232**, *228–229*, **390–391**, *390*
client-based troubleshooting tools, **856–859**, *857–860*
Client Check Detail tab, 284, *285*
Client Check node, **286**, *287*
Client Computer Communication Settings page, 139, *139*
client health, **266**, **273**
alerts, **268–270**, *269*, **287–288**, *288*
automatic remediation, **266–267**, *267*
determining, **267–268**, *268*
evaluation results, **283–286**, *284–285*
monitoring, **268**, **286–287**, *286–287*
overview, **273–274**
scheduled tasks, **274–275**, *274–275*
Actions page, **275**, *276*
CCMEval, **279–283**, *279*, *282*
Conditions page, **276**, *277*
History page, 278, *278*
Settings page, **277–278**, *277*
Triggers page, **275**, *276*
Client Language Selection page, 131
client.msi file, 176, 247, 256
Client Policy Polling Interval (Minutes) setting, 230
Client Policy Requests During The Following Days setting, 285
Client Policy settings, **229**, **391**
Client Push Installation Properties dialog box, 256, *256*
Client Push report, 590
Client Replace task sequence, 514
Client Status report, 590
Client Status History reports, 268
Client Status Settings Properties dialog box, 267–268, *268*, 284, *285*
Client Status Summary reports, 268
Client Time To Request Policy reports, 268
Client Troubleshooting Tool (CliSpy), 856–857, *857*
clients
application deployment, **339–342**, *340–342*
backing up, **799**
Compliance Settings, **627**, *627*
configuration baselines, **643–644**, *643*
deleted, **551–552**
health. *See* client health
information migration, 66
installation, **227**
boundaries, **244–246**, *245–246*
command-line properties, **247–252**
discovering network objects. *See* discovering resources
group policy, **257**
health, **266–271**, *267–270*
imaging, **258**
Linux/Unix, **259–262**, *260*
login scripts, **258**
Mac, **262–265**, *264*
manual process, **252–253**
push, **253–256**, *255–257*
settings, **227–232**, *228–229*
software distribution, **258**
software updates, **257**
supported operating systems, **232–234**
troubleshooting, **266**
verifying, **265–266**, *265*
inventory
processes, **550**
reports, **547**
log files, **835–836**
MIF storage location, **539**
migrating, 66, 86, **98–99**
notifications, **694–695**, *695*
planning, **59–60**
requirements, **24–32**
settings and deployment, **52**
default, **300–308**, *301–302*
hardware inventory, **529–530**
Software Metering, **560**, *561*
software update points, 381
software update settings, **392**, *392*
upgrades, **270–271**, *270*
CliSpy (Client Troubleshooting Tool), 856–857, *857*
Cloud Backup option, 753
cloud integration
distribution points, **215–216**, **222–225**, *223–224*
management certificates. *See* management certificates
overview, **213–214**
requirements, **214**
service certificates, **219–221**, *219–221*
Cloud page, 752–753, *752*
Cloud Services setting, 230
clusters, 49
cmclient.pkg file, 263
CMEnroll tool, **263–264**

CMtrace.exe program, 266, **361**, 646, **836**, *837*
CMTracelog utility, 156–157
Collect IDMIF files option, 539
Collect MIF files option, 539
Collect NOIDMIF files option, 539
Collected File Properties dialog box, 544, *544*
Collection Evaluation Viewer (CEViewer), **852–853**, *853*
collections, **14**, 53, **784**
  application deployment, **308**
  creating, **789–790**
  default, **785**
  deployment templates, 371
  enabling, 691
  migrating, **68–69**, **71–73**, *72–74*, **89–90**, *90*
  software inventory, **534–535**
  working with, **784**
Collections setting
  application deployment, **334**
  software update deployments, 428
Collections That Cannot Be Migrated dialog box, 71, *72*
columns in packages, 105
command line
  client installation properties, **247–252**, **260–262**
  WSUS 3.0 Administration Console installation, **402**
comments in application deployment, 335
Comments setting, 335
communications, site, **50**
Company Contact Information page, 735, *735*
Company Logo page, 735, *736*
company-owned device wipes, **769**
Company Resource Access feature, **656**
  certificate profiles, **656–660**, *657–660*
  reports, 590
  VPN profiles, **660–663**, *661–664*
  Wi-Fi profiles, **665–667**, *665–668*
Completion page
  distribution points, 173, *173*
  reporting role, 587
  secondary site servers, 147
compliance and Compliance Settings, 12, **623**
  clients, 230, **627**, *627*
  Company Resource Access feature, **656**
    certificate profiles, **656–660**, *657–660*
    VPN profiles, **660–663**, *661–664*
    Wi-Fi profiles, **665–667**, *665–668*
  configuration items. *See* configuration items (CIs)
  configuration packs, **647–648**, *648–650*
  new features, **624–625**, *624*
  overview, **623–624**
  purpose, **625**
  remote connection profiles, **654–656**, *655–656*
  reports, **646–647**
  software updates, **377–378**
  user data and profiles, **650–654**, *651–654*
Compliance and Settings Management reports, 590
Compliance Resource Access Manager role, 599, 775
Compliance Rules page, 634–635, *635*
Compliance Settings Manager role, 599, 775
Compliant status, 447
compmon.log file, 165
component servers, 46, **165**
Component Status folder, 177
Component Status messages, 838–839, *839*
computer accounts as administrators, 152
Computer Agent settings, **230–231**, **301–304**, *302*
computer client agents
  Asset Intelligence, 564
  settings, **227–232**, *228–229*, **390–391**, *390*
Computer Maintenance setting, 392–393
Computer Restart settings, 231, 304, *305*, 391
Computer Synchronization option, 709
computers
  information importing, **492–493**, *492*
  names, 242
  unknown, **495–497**, *495–496*
Computers for a Specific Console User report, 565
Computers With Multiple Users (Shared) report, 565
Conditions page, **276**, *277*
/config property, 249
ConfigMgr 10 registry key, 149, *150*
ConfigMgr Report Administrators group, 596
ConfigMgr Report Users group, 597
ConfigMgr Server option, 437
ConfigMgrAdminUISetup.log file, 101, 136
ConfigMgrAutoSave.ini file, 157
ConfigMgrBackup.ini file, 811, 817
ConfigMgrInstallation.adm template, 257
ConfigmgrMacClient.msi file, 263
ConfigMgrPostRecoveryActions.html file, 821, *822*
ConfigMgrPrereq.log file, 101, 126, 136
ConfigMgrSetup.log file, 136, 817
ConfigMgrSetupWizard.log file, 136, 817
ConfigMgrUnattendRecoverCAS.ini file, 819
configuration baselines, 631
  clients, **643–644**, *643*
  initial, **639–640**
  options, **644**
  rules, **640–644**, *641*, *645*
configuration items (CIs)
  Compliance Rules page, **634–638**, *635*
  creating, **628–629**
  Detection Methods page, **631–632**, *632*
  General page, **628–630**, *628*, *630*
  Settings page, **632–634**, *633*, *635*
  Summary page, **638**, *638*
  types, **625–626**

Configuration Manager Client Will Force A Mandatory Device Restart option, 331
Configuration Manager console
certificate profiles, 658
user data and profiles, 651
Configuration Manager overview
Active Directory schema, **37–38**
client notifications, 694–695, *695*
client settings and deployment, **52**
cloud communication, 215
console upgrading, **100–101**
content management, **52–53**
deployment, **60–63**
intelligence gathering, **21–23**
migration needs, **23–24**
troubleshooting, **845**
disaster recovery, **56**
environment design, **56–61**
hierarchies and sites, **38–44**, *38*, *44*
Mac client installation, 262–264, *264*
major features, **12–20**, *13*
migration, **54–56**
mobile devices. *See* device settings management for mobile devices
resource discovery, **51–52**
role-based administration, **53–54**
site boundaries and boundary groups, **44–45**
site communications, **50**
site security mode, **51**
site system design, **47–49**
site system roles, **45–47**
SQL considerations, **49–50**
SSRS installation, **588**
system requirements, **24–36**
Windows Intune, 731, *732*
Configuration Manager Properties dialog box, 560, *561*, 644, *645*
Configuration Manager Status Message Viewer window, 840, *840*
Configuration Manager Trace Log Viewer tool, 857
configuration.mof file, **529–530**, **541**, *541*
configuration packs, importing, **647–648**, *648–650*
configuration settings, migrating, **77–78**
Configure Automatic Updates option, 393
Configure Client Setting dialog box, 543–545, *544*, *546*
Configure ConfigMgr Integration dialog box, 511, *511*
Configure Manager Alerts option, 433
Configure Network page, 484, 518
Configure The Network page, 493
Confirm Object Delete dialog box, 558
Confirm Settings page, 674
Confirmation page
configuration packs, 649, *650*
System Center Updates Publisher, 443, *443*
Connect-MsolService command, 731
Connection page
mobile devices, 765–766, *766*
VPN profiles, 661, *662*
connectors for Windows Intune, **731–737**, *732–737*
connectorsetup.log file, 772
Console Users on a Specific Computer report, 565
content
library, **42–43**
backing up, **799**
software updates, 366
managing, **52–53**
migrating, 66
prestaging, **43**
replicating, 50
validating, **43**, *44*
distribution points, 171–172, *172*, **294**
secondary site servers, 145, *146*
Content Library Explorer, **853**, *854*
Content Library Transfer tool, 854, *855*
Content Location settings
application deployment type, 325
operating system images, 456
operating system installers, 456
Content Locations settings
boot images, 454
sample application, 321, *322*
Content Ownership Tool, 855, *855*
Content page
application deployment type, 325, *325*
Deploy Software Wizard, 335, *335*
Content Rating page, 751–752, *751*
Content Validation page
distribution points, 171–172, *172*, **294**
secondary site servers, 145, *146*
contentwebrole.cspkg file, 224
Continual Service Improvement phase, **4–5**
Converted package conversion state, 106
Cookies option, 749
copying backups to other locations, **802**
COUNT command, 612
Create A Deployment Alert When The Threshold Is Higher Than The Following option, 339
Create A Deployment Alert When The Threshold Is Lower Than The Following option, 338
Create A New Custom Task Sequence task, 457
Create A New Deployment Package option, 425
Create A New Task Sequence page, 483
Create Antimalware Policy dialog box, 679–685, *680–685*
Create Application Wizard, 309, *309*, **311–314**, *311–313*, 323–324, **333–339**, *334–338*
Create Automatic Deployment Rule Wizard, 389
Create Boot Image Using MDT dialog box, 512, *512*
Create Certificate Profile Wizard, 658–660, *658–660*
Create Cloud Distribution Point Wizard, 222–224, *223*
Create Configuration Baseline Wizard, *638*, 639–640

Create Configuration Item Wizard
Compliance Rules page, **634–638**, *635*
Detection Methods page, **631–632**, *632*
General page, **628–630**, *628*, *630*
mobile devices, 743, *743*
Automatic VPN page, 766, *767*
Browser page, 748–749, *750*
Certificate Properties page, 764, *764*
Certificates page, 758–759, *758*
Cloud page, 752–753, *752*
Connection page, 765–766, *766*
Content Rating page, 751–752, *751*
Device page, **745–747**, *746*
Email Management page, 747–748, *747*
Encryption page, 756–757, *756*
General page, 743–744, *743*
Internet Explorer page, 749–751, *750*
Mobile Devices Settings page, 743–744, *744*
Password page, **744–745**, *744*
Peak Synchronization page, 754, *755*
Platform Applicability page, 761–762, *762*
Roaming page, 754, *755*
SCEP Enrollment page, 763, *763*
Security Configuration page, 768, *769*
Security page, 753–754, *753*
Store page, 747–748, *748*
Summary page, 765
Supported Platforms page, 761, *761*
System Security page, 759–760, *759*
Trusted Root CA Certificate page, 762, *763*
Wi-Fi Profile page, 767, *768*
Windows Server Work page, 760, *760*
Wireless Communications page, 757–758, *757*
Settings page, **632–634**, *633*, *635*
Summary page, **638**, *638*
Create Custom Client Device Settings dialog box, 397, *397*, 676–678, *677*
Create Deployment Type option, 316
Create Enrollment Profile window, 263
Create MDT Task Sequence dialog box, 513–515, *513*, *515*
Create New Task Sequence page, 493
Create Package and Program Wizard, 354, *354*, 506–507, *507*
Create Prestage Content File option, **316**, *316*
Create Prestage Content File Wizard, 316, *316*
Create Remote Connection Profile Wizard, 655–656, *655–656*
Create Rule dialog box, 636–637, *637*
Create Secondary Site Wizard, 141–147, *142–146*
Create Setting dialog box, 632–634, *633*
Create Site System Server Wizard, distribution points, 166–173, *166–173*
Create Software Metering Rule Wizard, 556–557, *557*
Create Subscription Wizard, 609, *610*
Create Task Sequence Media Wizard, 496, *496*, 504–505, *504–505*
Create Task Sequence Wizard
bare-metal machines, 493–494, *494*
for deployment, 484–487, *484–487*
media boot, **475–476**, *475–477*
PXE boot, 471–474, *472–473*
virtual hard drives, 517
Create User Data And Profiles Configuration dialog box, 651–654, *652–654*
Create Virtual Environment dialog box, 349, *350*
Create Virtual Hard Disk Wizard, 517, *518*
Create VPM Profile Wizard, 661–664, *661–664*
Create Wi-Fi Profile Wizard, 665–667, *665–668*
Create Windows Intune Subscription Wizard, 731–736, *733–736*
Credentials Synchronization option, 753
criteria for update searches, **421–423**, *422–423*
custom labels, **567**
Custom Schedule dialog box
hardware inventory, 538
network discovery, 243, *244*
custom security scope, **779–781**, *779*
Custom Severity page, **389–390**
Customer Experience Improvement Program page, 133
customer service, **11**
Customizations tab, 454
customized boot images, 77

D

dashboards
migration, 84, *84*
package conversion, 105, *106*, 111
status messages, 838, *839*
Data Access tab
boot images, 454
operating system images, 456
operating system installers, 456
data gathering in migration, 66, **68**, **86–88**, *87*, **102**
Data Gathering Status dialog box, 86, *87*
data library, 42
Data Preview page, 493, 516
Data Replication Service (DRS), 845–846, **848–849**, *849*
Data Roaming option, 756
data source and Data Source tab
authentication accounts, 587
boot images, 454, 467, *467*
operating system images, 455
operating system installers, 456
report properties, **604**
data types, **847–848**, *848*
Database Information page, 132, *132*, 138, *138*, 814, *814*

Database Replication
troubleshooting, **845–849**, *846*, *848–849*
databases
moving, **823–824**, *824*
validating, **153**, *154*
dataldr.log file, 551
DataLib folder, 174–176, *175*
Date Published setting, 320
dcmagent.log file, 646
Deadline Behavior setting, 431
Default Actions page, 682, *682*
Default Application Catalog Website Point setting, 230, 391
Default Browser option, 749
Default Client Malware Policy, 687
Default security scope, 778
Default Settings dialog box
BITS, 300, *301*
Computer Agent, **301–304**, *302*
Computer Restart, 304, *305*
Endpoint Protection, 676, *676*
inventory, 533, *534*
Software Deployment, 304, *305*
software inventory, 542, *543*
User and Device Affinity, 306, *306*
defaults
client settings, **300–308**, *301–302*, 627, *627*
collections, **785**
hardware inventory, **541–542**
MIF storage location, **539**
define and capture phase in migration, 82
definition files in SCEP, **687–690**, *688–689*
Definition Updates page, 685, *685*
Delete option, **317**
deleted clients, **551–552**
deleting
applications, **317**
software metering rules, **558**
Deliver phase, MOF, **10**
delta discovery, 242
delta inventory information, 528
Delta Synchronization Interval option, 707
dependencies and Dependencies tab
Application Deployment
Application References, **296**, **298**
BITS-enabled IIS, 300
configuring, **345**, *345*
default client settings, **300–308**, *301–302*
distribution points, **299–300**
management points, **299**
types, 333, *333*
Asset Intelligence, 572
Deploy Configuration Baselines Wizard, 643–644, *643*
Deploy Software Updates Wizard
languages, 387
packages, **372–373**
settings overview, **373**
software updates, 389, **427–434**, *429–432*
Deploy Software Wizard
Alerts page, **338–339**, *338*
Content page, 335, *335*
Deployment Settings page, 336, *336*
General page, **333–335**, *334*
operating system image capturing, 477–479, *478–479*
Scheduling page, 337, *337*
task sequences, 487–488, *488*
User Experience page, 337–338, *337*
deploy stage, **11**
Deploy User Data and Profiles Configuration Policy dialog box, 650–651, *651*
deployment
application. *See* Application Deployment
clients, **52**
Configuration Manager, **60–63**
images, **483**
intelligence gathering, **21–23**
migration needs, **23–24**
operating system. *See* operating system deployment (OSD)
packages, **372–373**, 424–427
SCEP, **670**
software updates, **373–374**, **378–380**
downloading, **424–427**, *424*, *426*
finding, **420–423**, *421–423*
groups, **427**
monitoring, **445–449**, *445–448*
rules, **374–376**, *375*
templates, **371–372**
status messages, **841–842**
task sequences, **487–491**, *488–491*
troubleshooting, **845**
Deployment Deadline settings, 230
Deployment Image Servicing and Management (DISM), 520
Deployment Monitoring Tool, 857–858, *857*
Deployment Name setting, 428
Deployment Options setting, **326**
Deployment Package page
Deploy Software Updates Wizard, 434
software updates, 424, *424*
deployment phase in migration, 82
Deployment Settings page, 336, *336*, 488, *488*
Deployment Status window, 490, *491*
Deployment Types tab, 308–309, 321, *322*, 324
Deployments node, **358–359**, *359*
depth management of mobile devices, **199**, **702**, **715–716**
device enrollment, **721**
administrator configuration, **721–722**, *721–722*
user configuration, **722–728**, *723–727*
roles
Application Catalog web service point, **720**, *721*
distribution point, **720**, *720*
enrollment point, **717–718**, *717*
enrollment proxy point, **716–717**, *716*
management point, **718–719**, *718*
Microsoft enterprise certification authority, **719**, *719*
Windows Intune, **728–730**, *729–730*
DESC keyword, 612
descriptions
configuration items, 629, 634
deployment packages, 425
software metering rules, 557
design, site system, **47–49**
Detail Level setting, 429

Detection Method page, **297**, **328**, *328*, **346**, **631–632**, *632*
Detection Rule dialog box, 328, 353, *353*
Determine Behavior Based On Return Codes option, **331**
device drivers, **459**, **497–499**, *497–499*
device enrollment, **721**
  administrator configuration, **721–722**, *721–722*
  user configuration, **722–728**, *723–727*
Device Management reports, 590
Device page, **745–747**, *746*
Device Restart Behavior setting, 431
device settings management for mobile devices, **742**
  Automatic VPN page, 766, *767*
  Browser page, 748–749, *750*
  Certificate Properties page, 764, *764*
  Certificates page, 758–759, *758*
  Cloud page, 752–753, *752*
  Connection page, 765–766, *766*
  Content Rating page, 751–752, *751*
  Device page, **745–747**, *746*
  Email Management page, 747–748, *747*
  Encryption page, 756–757, *756*
  General page, **743–744**, *743*
  Internet Explorer page, 749–751, *750*
  Mobile Devices Settings, 743–744, *744*
  Password page, **744–745**, *744*
  Peak Synchronization page, 754, *755*
  Platform Applicability, 761–762, *762*
  Roaming page, 754, *755*
  SCEP Enrollment page, 763, *763*
  Security page, 753–754, *753*
  Security Configuration page, 768, *769*
  Store page, 747–748, *748*
  Summary page, 765
  Supported Platforms, 761, *761*
  System Security, 759–760, *759*
  Trusted Root CA Certificate page, 762, *763*
  Wi-Fi Profile page, 767, *768*
  Windows Server Work, 760, *760*
  Wireless Communications, 757–758, *757*
Devices For Certificate Enrollment option, 764
DHCP with PXE, 465
Diagnostic Data Submission option, 747
-dir property, 260
Direct Push When Roaming option, 712
Direct Rule type for collections, 784
Disable Alternate Sources option, 231
DisableCacheOpt property, 250
DisableSiteOpt property, 250
disabling
  password change requirements, **731**
  software metering rules, **555–556**
disaster recovery, **56**, **797**
  backups, **801–807**, *803*, *806*
  central sites, **811–817**, *812–816*
  maintenance options, **819–821**
  monitoring, **817**, *817*
  multisite environments, **818**
  planning, **797–798**
  post-recovery tasks, **821–822**, *822*
  restores, **807–810**, *809*
  starting, **811**
  unattended, **818–819**
discovering resources
  Active Directory, **235–237**, *236–237*
    forests, **237–238**, *238*
    groups, **240**, *241*
    heartbeat, **240–242**, *243*
    network, **242**
    scheduling, **242–243**, *243–244*
    system, **239**, *239*
    users, **240**
  Add Exchange Server Wizard, **707–708**, *708*
  out-of-band management, **17**
  overview, **234–235**
Discovery page, **707–708**, *708*
disk space, 845
Disks category, 458
DISM (Deployment Image Servicing and Management), 520
dismgr.log file, 772
Display in Software Center option, 338
Display Name Properties window, 545, *545*
display names for software inventory, **534–535**, 545, *545*
Display This As A Featured App option, 321
distmgr.log file, 177, 465
Distribute Content option, **318**
Distribute Content Wizard, 483
Distribute The Content For This Package To Preferred Distribution Point option, **425**
distribution
  boot image packages, **466–467**
  images, **483**
  software. *See* software distribution
Distribution Point page, 144, *144*, **166–168**, *167*
distribution point role, 46, **720**, *720*
distribution points, **41–44**, *44*, **165–176**, *166–176*
  changes, **293–296**
  cloud integration, **215–216**, **222–225**, *223–224*
  dependencies, **299–300**
  high availability, 49
  managing, **52**
  migrating, 66, **79–80**, **83**, **85**, **88–89**
  operating system deployment, **455**, 489
  operating system support, **34–36**
  PXE on, **464–465**, *465*
  reassigning, **85**
  software requirements, **177**
  software updates, 425
  status messages, **844**
  troubleshooting, **177**, *177*
  upgrading, **93–98**, *94–95*, *97*
Distribution Points page, 425, 489
Distribution Priority setting, **425**
Distribution Settings page
  boot images, 454
  operating system images, 456
  operating system installers, 456

sample application, 321, *322*
software updates, 425, *426*
distributions
package migration, **75**
status messages, **843**
.dmg files, 352, *353*
dmpdownloader.log file, 772
dmpuploader.log file, 772
DNSSUFFIX property, 251
Do Not Expire A Superseded Update Until The Software Update Is Superseded For A Specified Period option, 406, 413
Do Not Synchronize From Microsoft Update Or The Upstream Update Server option, 405
Do Not Synchronize From Microsoft Update Or Upstream Data Source option, 412
Document Synchronization option, 753
domains
profiles, 686
Windows Intune, **728–729**, *729–730*
Download Location page, 378, 426–427, 434
Download Only Content Changes To The Distribution Point option, 426
Download Settings For Non-preferred Distribution Points settings, 433
Download Settings For Slow Or Unreliable Network settings, 433
Download Settings page, 372
Download Software Updates From A Location On My Network option, 426
Download Software Updates From The Internet option, 426
Download Software Updates Wizard, 387, 424–427, *424*, *426*
Download Updates Software Wizard, 369
downloading software updates, **424–427**, *424*, *426*
/downloadtimeout property, 248
DP Job Manager, **852**, *852*
drive letters for images, 487, *487*
Drive Settings page
distribution points, 168–169, *168*
secondary site servers, 145, *145*
drive space requirements for clients, 25
Driver Details page, 498
drivers, device, **459**, **497–499**, *497–499*
Drivers category for task sequences, 458
Drivers tab for boot images, 454
DRS (Data Replication Service), 845–846, **848–849**, *849*
Duplicate Template dialog box, 219

E

Edit Device Ownership dialog box, 769, *769*
Edit Inventory Classes dialog box, 576, *576*
Edit Primary Devices node, 357, *358*
Editions tab, 456
EICAR test malware, **695–699**, *696–698*
email
alerts, **692–693**, *693*
mobile devices, **711–712**, *711*, 747–748, *747*
report subscriptions, **610–611**
Email Attachments option, 712
Email Download While Roaming option, 754
Email Management page, 747–748, *747*
Email Management Settings page, **711–712**, *711*
embedded devices, 432
Empower Users feature, 365
Enable Automatic Site-wide Client Push Installation option, 254
Enable Certificate Templates dialog box, 220
Enable Hardware Inventory On Clients option, 538
Enable Software Updates on Clients option, **397**
Enable System Center Operations Manager Maintenance Mode option, 339
enabling
Asset Intelligence, **575–576**, *577*
collections, 691
Software Metering Client Agent, 553
software metering rules, **555–556**, *556*
Encrypted Backup option, 753
encryption and Encryption page
client inventory reports, **547**
mobile devices, 756–757, *756*
endpoint protection. *See* System Center Endpoint Protection (SCEP)
Endpoint Protection client agent, **675–679**, *676–677*
Endpoint Protection Manager role, 776
Endpoint Protection Point role
adding, **209–210**, *209*
configuring, **672–675**, *674*
description, 46
reports, 599
EndpointProtectionAgent.log file, 695
Enforcement phase in software updates, 448
enrollment, device, **721**
administrator configuration, **721–722**, *721–722*
mobile devices, **737–741**, *738*, *740–742*
user configuration, **722–728**, *723–727*
Enrollment Point Connection Account option, 718
enrollment point role, 46, **717–718**, *717*
Enrollment Point setting, 716
Enrollment Profile window, 263
enrollment proxy point role, 46, **199–203**, *201–202*, **716–717**, *716*
Enrollment setting, 231
EnrollmentService.log file, 771
EnrollmentWeb.log file, 771
Enrollsrvmsi file, 203
Enrollsvc.log file, 203
Enrollweb.log file, 203
Enrollwebmsi file, 202
Entended Key Usage option, 765
Enter A Password To Access The Application Store option, 748
environment variables, **634**
EPCtrlmgr.log file, 210, 675
EPMgr.log file, 210, 674–675

EPsetup.log file, 210, 675
Error Lookup window, 836, *837*
Error status
in-console monitoring, **446–447**
package conversion, 106
Estimated Install Time (Minutes) option, 330
Evaluation phase in software updates, 448
event logs, **565–566**
Exclude Collections Rule, 784
Excluded Settings page, 683, *683*
excluding
malware scanning items, 683, *683*
software inventory files, **547–548**, *548*
expired software updates, 365
Explicit Content In Media Store option, 752
Export Application Wizard, 318–319, *318*
exporting
applications, **318**, *318*
management certificates, **216–219**, *217–218*
reports, **621**
service certificates, **220–221**, *220–221*
software updates, 76
synchronization with, **418–419**
extending hardware inventory, **540–542**, *541*
ExtractContent.exe file, 818

F

fallback, 173
fallback status point role, 46–47, **189–191**, *190*
fat images, 460
FEP (Front Endpoint Protection) vs. SCEP, **669**
file-based report subscriptions, **609**, *610*
file collection for software inventory, **534**
File Encryption On Mobile Device option, 756
File Encryption On Mobile Devices option, 713
file formats for management certificates, 216, *217*
file library, 42
file system validation, **150**, *151*
FileLib folder, 174, 176, *176*
files for software updates, **369**
FileSystemFile.log file, 547, *548*
filters
embedded devices, 432
software updates, **364**
financial management, **8**, **11**
Find All Mobile Devices In The Exchange Organization option, 708
finding
management points, **180–181**
software updates, **420–423**, *421–423*
firewalls, **685–686**, *686*
flat hierarchies, **774**
folder migration, **78**
Folder Redirection screen, 651, *652*
/forcereboot property, 248
forest discovery, 52, **237–238**, *238*
Foxit Reader Properties dialog box, **319–333**, *319–320*, *322–325*
FQDNs (fully qualified domain names), 225
Fraud Warning option, 749
free drive space requirements for clients, 25
Front Endpoint Protection (FEP) vs. SCEP, **669**
Fryer, Andrew, 2
FSP property, 251, 260
fspMSI.log file, 191
Full Administrator role, 599, 776
full antimalware scans, 680
Full Content update option, 442
Full Synchronization Schedule option, 707
fully qualified domain names (FQDNs), 225

G

general configuration items, **642**
General Information page, **313–314**, *313*
application deployment, 309, *309*
sample application, 319–320, *319*
General Items page, 324, *324*
General License Statement, **580–581**, *580*
General settings
Add Exchange Server Wizard, **705–706**, *706*
boot images, 453–454, *453*
client push installation, 254, *255*
configuration items, **628–630**, *628*, *630*, 632, *633*
Create Application Wizard, 311–312, *311*
Deploy Software Updates Wizard, 428–429, *429*
Deploy Software Wizard, **333–335**, *334*
mobile devices, 743–744, *743*
operating system images, 455
operating system installers, 456
reports, **602**
sample application, *319*
SCEP, 673
secondary site servers, 142–143, *143*
site system roles, 162, *162*
software metering, 554–557, *555*, *557*
software updates, **384–385**
state migration points, 462
synchronization points, 577
task sequences, 457, 487
Windows Intune, 732, *732*
General Settings window, **709**, *709*
Generate System Center Operations Manager Alert When A Software Installation Fails option, 339
Getting Started page
central administration sites, 129, *129*
primary sites, 136–138, *137*
global conditions in migration, 75
Global Conditions node, 347, *349*
global data replication, 50, 847, *848*
global roaming, 37
Go To Intranet Site For Single Word Entry option, 751
goals
determining, **22–23**
software updates, **380**
governance, 12
group policies and GPOs
client installation, **257**
SCEP, 673
settings, **393**

groups
Active Directory, 52, **240**, *241*
boundary, **44–45**
distribution points, **52**, **294–295**, **844**
software updates, **364**, 370, **427**
validating, **151–152**, *152*
GUIDs for cloud distribution points, 225

H

hard drives, virtual, **516–517**
creating, **518–519**, *518–519*
managing, **519–522**, *520–522*
task sequences, **517–518**
hardware inventory, **528–529**
client settings, 231, **529–530**
configuration.mof file, **529–530**
configuring, **537–540**, *538*
extending, **540–542**, *541*
MIF files, **532–533**
Registry, **541–542**
reporting classes, **530–532**
troubleshooting, **550**
Hardware Inventory Client Agent, 564
Hardware Inventory During The Following Days setting, 285
Hardware Inventory option, 231
hardware reports, **572–573**, 590
hardware requirements
Asset Intelligence, **568**
clients, **25**
Hash Algorithm option, 765
health, client. *See* client health
heartbeat discovery, 51, **240–242**, *243*, 548
Heartbeat Discovery During The Following Days setting, 285
hidden reports, 602
hierarchies, **38**, *38*
central administration sites, **38–39**
design and implementation, **124**
distribution points, **41–44**, *44*
flat, **774**
planning, **58–59**
primary sites, **39–40**
secondary sites, **40–41**
software update points, **380–381**
Hierarchy Maintenance tool, **819–821**
high availability, **49**
history and History page
reports, 607–608
SCEP, 697, *697*
scheduled tasks, 278, *278*
HTTP option, 719
HTTP security mode, 51
-httpport property, 261
HTTPS option, 719
HTTPS security mode, 51
-httpsport property, 262
Hyper-V Manager, 518, *518*

I

Icon option, 321
Identification registry key, 148, *149*
Idle Time Before Mobile Device Is Locked setting, 745
Idle Time In Minutes Before Mobile Device Is Locked setting, 711
IDMIF files
description, **532–533**
storage location on clients, **539**
If Software Updates Are Not Available On Preferred Distribution Point settings, 433
If The Running Task Does Not End When Requested, Force It To Stop option, 278
Ignore Mobile Devices That Are Inactive For More Than (Days) setting, 708
-ignoreSHA256validation property, 262
Image Capture Wizard, 481, *481*
Image Destination page, 481, *481*
Image Information page, 481
images
boot. *See* boot images
client installation, **258**
creating, **471–476**, *472–477*
drive letters, 487, *487*
Microsoft Deployment Toolkit, **512–513**, *512*
offline servicing, **520–522**, *521–522*
operating system, **455–456**
automatic building and capturing, **477–480**, *478–480*
deploying, **482–483**
reference computers, **480–481**, *481–482*
task sequences, 458
Images tab
boot images, 454
operating system images, 455
Immediately Expire A Superseded Update option, 406, 413
Import Certificate dialog box, 759, *759*
Import Computer Information Wizard, 492, *492*
Import Configuration Data Wizard, 649, *649–650*
Import Information page, 312, *312–313*
Import New Driver Wizard, 498–499, *498–499*
Import Software License Wizard, 578–580, *578*, *580*
Import User Device Affinity Wizard, 355, *356*
importing
application information, 312, *312–313*
certificates, 759, *759*
computer information, **492–493**, *492*
configuration packs, **647–648**, *648–650*
drivers, 498–499, *498–499*
reports, **603**, **620–621**
software licenses, **578–581**, *578*, *580*
software updates, 77, **439**, *440*
update synchronization with, **418–419**
user device affinity, 355, *356*, **502**, *502*
In-App Purchases option, 748
in-band management, 17
in-console software updates deployment monitoring, **445–448**, *445–448*
In Progress status, 447
Inactive Client Details reports, 268
incident management function, **6**
Include Collections Rule, 784
Include Updates page, 485, 494
Infrared option, 713
Infrastructure Administrator role, 599–600, 776

Install An Existing Image Package task sequence, 457
Install Applications page, 486, *486*, 494
Install Configuration Manager Client Wizard, 256, *257*, 485, 518
Install Endpoint Protection Client In Client Computers option, 231
Install page, 135, *135*, 816, *816*
Install Permissions settings, 230
Install Profile dialog box, *739*
Install script, 259
Install The Configuration Manager Client page, 494
Install The Windows Operating System page, 493, 518
INSTALL.WIM file, 468–469, 487
Install Windows page, 483, *484*, *486*
installation
client. *See* clients
site system roles, **160–163**, *161–162*
software update points, **382–384**
System Center Updates Publisher, **436**, *436*
WSUS, **398–401**
Installation Behavior setting, **329**
Installation Deadline setting, 430
Installation Program setting, 327
Installation program visibility settings, **330**
Installation Progress window, 481, 489, *489*
Installation Properties tab, 256, *256*
Installation Source Files page, 142–143
Installation Start In option, 327
Installed Updates tab, 456
installers, operating system, **456**
instances, SSRS, 585
Intel Activity Management Technology, 17
interaction of site system roles, 160–161
Internet-based clients for software update points, **381–382**
Internet Explorer page, 749–751, *750*
Internet FQDN setting, 403, 407
Internet option for software updates, 434
Internet Sharing From Mobile Devices option, 709
interoperability with Configuration Manager 2007, **80**
intranet-based clients for software update points, 381
Intranet Security Zone option, 751
Inventoried Software Titles node, **567–568**
inventory, **13**, **527–528**
hardware. *See* hardware inventory
scheduling, **536–537**
software
collecting, **533–535**, *534*
configuring, **542–550**, *543–545*
troubleshooting, **550–552**
viewing, **535–536**, *535*, **545–546**, *546*
Inventory Reporting Detail setting, 542
InventoryAgent.log file, 550–552
IP address ranges, 44
IP subnets, 44
IPv6 prefix, 44
IT Infrastructure Library (ITIL), **2–9**
IT Operations Management function, **6**
IT Service Continuity Management process, **8–9**
IT service management (ITSM), **1–2**
ITIL, **2–9**
MOF, **9–12**
IT Service Management Forum (itSMF), 2

J

jobs, migration, *66*, **84**, **89–92**, *90–92*

K

-keepdb property, 261
Key Size (Bits) option, 765
Key Storage Provider (KSP) option, 764
Key Usage option, 765
keys for management certificates, 216–218, *217–218*
Keywords option, 321

L

labels in Asset Intelligence, **567**
Language Selection page, 387, 427, 434
languages
deployment, 325, 372
software metering rules, 557
software updates, **387**, 415, *416*, 434
Languages page, 207, 387, 415, *416*
LaunchMedia.cmd command, 480
legacy boot images, **522–523**
libraries
content, **42–43**
ITIL, **2–9**
licenses
Asset Intelligence, **578–581**, *578*, *580*
central administration sites, 130
reports, **574–575**
link states, **846**
Link Text option, 321
linked reports, **619**
Linux operating system
application deployment, **354–355**, *354*
client installation, **259–262**, *260*
client support, 234
support for, **30–32**
Linux/Unix Configuration Manager, 259
lite management of mobile devices, **199**, **702**
Account page, **707**, *707*
configuration results, **714–715**, *714–715*
Discovery page, **707–708**, *708*
General page, **705–706**, *706*
Settings page, **708**
Application settings, **713**, *714*
Email Management settings, **711–712**, *711*
General settings, **709**, *709*
Password settings, **709–710**, *710*
Security settings, **712–713**, *713*
load balancing, **49**
local installation, **128**
Localized Application Name option, 321
Localized Description option, 321
Locate Driver page, 497, *497*
locations for deployment templates, 372

log files
application deployment, **360–361**
backup process, **804**
client, **835–836**
client notifications, 695, *695*
management points, **182–183**, **834–835**
SCEP, 675
site servers, **832–834**
for troubleshooting, **832–837**
Windows event, **565–566**
login scripts, **258**
/Logon property, 248
Logon Requirement option, **329**
logos, reports, 595–596, *596*

M

Mac Computer Enrollment Wizard, 264, *264*
Mac operating system
application deployment, **352–354**, *353*
client installation, **262–265**, *264*
client support, 234
support, **29**
Macclient.dmg file, 263
maintenance plans, **827–831**, *828*
maintenance windows, **387–389**, *388*
malware, **670**
antimalware policy, **679–685**, *680–685*
assigning policy, 687, *687*
scenario, **695–699**, *696–698*
Windows Firewall policies, **685–686**, *686*
Malware Detection alerts, 690
Malware Outbreak alerts, 690
Manage Administrative Categories dialog box, 630, *630*
Manage Endpoint Protection Client On Client Computers option, 231
Manage layer for MOF, **10**
management certificates, **215**
creating, **216–218**, *216–217*
exporting, **216–219**, *217–218*
uploading, **222**, *222*
Management information format (MIF) files, **532–533**, **539**
Management Point page, 179, *179*
Management Point Database page, 179, *180*
management point role, 47, **718–719**, *718*
management points
dependencies, **299**
finding, **180–181**
high availability, 49
inventory, **550**
log files, **182–183**, **834–835**
overview, **178–179**, *179–180*
proxy, **180–181**
queries, **182**
server locator point functionality, **182**
software requirements, **183**
troubleshooting, **183**
Manual package conversion state, 105
manual synchronization, 377
Manually Copy The Content In This Package To The Distribution Point option, 426
Manually Define This Information option, 312
MAPS (Microsoft Active Protection Service), **670–671**, *671*
Maximum Allowed Run Time (Minutes) setting, **330**
Maximum Custom MIF File Size (KB) setting, 539
Maximum Run Time settings, **388–389**
Maximum Size For HTML Email (Automatically Downloaded) setting, 748
Maximum Size For Plain Text Email (Automatically Downloaded) setting, 748
Maximum Size Of An Attachment (Automatically Downloaded) setting, 748
Maximum Time To Keep Calendar Entries setting, 712
Maximum Time To Keep Email setting, 712, 748
MDT. *See* Microsoft Deployment Toolkit (MDT)
media boot task sequences, **475–476**, *475–477*
Media Properties page, 504, *504*
media task sequences, **459**
Media Type page, 475, *476*, 496
memory
central administration sites, 135
SQL, 128, 135
messages. *See* status messages
metadata in software updates, **368–369**, 414, 419, 442
Metadata Only option, 442
Metered Internet Connections setting, 231
metering software. *See* Software Metering feature
Microsoft Active Protection Service (MAPS), **670–671**, *671*
Microsoft Active Protection Service page
antimalware policy, 684, *684*
Endpoint Protection Point role, 209, *209*
Microsoft Application Virtualization Management, **18–19**
Microsoft Calculator Plus utility, 628–629
Microsoft Certificate Service, 262
Microsoft Configuration Manager folder, 150, *151*
Microsoft Deployment Toolkit (MDT)
backing up, 800
boot images, **512–513**, *512*
installing, **510–511**
integrating, **511**, *511*
scenarios, **510**
task sequences, **513–515**, *513*, *515*
Microsoft enterprise certification authority role, **719**, *719*
Microsoft Malware Protection Center (MMPC), 670
Microsoft Operations Framework (MOF), **9–10**
Microsoft Software License Terms page, 130
Microsoft Update catalog, 376
Microsoft Volume License Statement, **578–579**
MIF (Management information format) files, **532–533**, **539**
migmctrl.log file, 84, 94

migration, **65**
data-gathering process, **68**
distribution points, **79–80**
introduction, **66–67**
needs, **23–24**
objects, **54–56**
not supported, **79**
supported, **72–79**, *72–74*
packages, **103**
best practices, **110**
monitoring, **110–111**, *111*
Package Conversion Manager, **103–104**, *104*
process, **104–110**, *106*, *108–109*
planning, **81–82**
post-migration considerations, **101–102**, *102*
preparing, **81**
report, 591
side-by-side. *See* side-by-side migration
source hierarchy, **67–68**, *67*
types, **68**
wipe-and-load, **100**
migration data, backing up, 800
migration points, **186–189**, *186–188*, **462–464**, *463*
Minimum Password Length (Characters) setting, 710
MMPC (Microsoft Malware Protection Center), 670
mobile device and AMT enrollment point role, **199–203**, *201–202*
Mobile Device Management dialog box, 739
Mobile Device Management While Roaming option, 754
mobile devices, **16**, **701**
depth management. *See* depth management of mobile devices
device settings management. *See* device settings management for mobile devices
lite management. *See* lite management of mobile devices
management overview, **702–704**
new features, **701–702**
operating systems, **31**
troubleshooting, **771–772**
wipe vs. selective wipe, **769–771**, *770–771*
Mobile Devices Settings page, 743–744, *744*
models, report, **613**
modes, SSRS installation, 585
Modify Virtual Hard Disk Wizard, 519, *520*
MOF (Microsoft Operations Framework), **9–10**
monitoring, **53**
application deployment, **358–359**, *359*
client health, **286–287**, *286–287*
client status, **268**
distribution point upgrades, 94, *95*
migration, 66, **84**, *84*
offline servicing, **522**, *522*
package conversion, **110–111**, *111*
recovery, **817**, *817*
SCEP, **672**
software updates, **364**, **445–449**, *445–448*
Movie Rating option, 752
moving
applications, 318
reports, **619**
site databases, **823–824**, *824*
MP_Hinv.log file, 551
MP property, 248, 260
mpcontrol.log file, 183
mpMSI.log file, 183
mpSetup.log file, 183
msoidcli_64bit.msi file, 730
mtrmgr.log file, 560, *561*
multicast support and Multicast page, **42**, 170–171, *171*
Multiplayer Gaming option, 747
multiple malware detection alerts, 690
multiple product updates, 369
multisite environments, recovery in, **818**

N

names
cloud distribution points, **225**
computers, 242
configuration items, 629
deployment, 325, 428
management certificates, 218
packages, 425
servers, 162
software inventoried products, **534–535**
software metering rules, 557
Namespaces For Intranet Zone option, 751
native uninstall support, **297**
Netdisc.log file, 242
Network Access Account page, 307, *307*, **461–462**, *462*
Network Access Protection (NAP), **16**
Active Directory schema, 37
compliance, 232
report, 591
system health validator, 185
Network Firewall option, 760
Network Load Balancing (NLB), 382
Network Location option, 434
Network report, 591
networks
connectivity, 845
describing, **23–24**
discovery. *See* discovering resources
software updates, 434
speed, 45
New Site Role Wizard, 577
New Table Or Matrix Wizard, 615
New Task Sequence Wizard, 483, 493
NLB (Network Load Balancing), 382
no_sms_on_drive.sms file, 168
No Specific Action deployment option, 331
NoCRLCheck property, 248, 261
NOIDMIF files
description, **532–533**
location, **539**
Nokia operating system for mobile device management, 703
non-task sequence bootable media, **116–119**, *117*
noservice property, 248, 261
Not Applicable package conversion state, 105, **109**
Notification Manager, 694–695
notifications, client, **694–695**, *695*

Number Of Failed Logon Attempts Before Device Is Wiped setting, 711
Number Of Passwords Remembered setting, 711

O

objects
content-related, **53**
discovering. *See* discovering resources
migrating, **54–56**, 66, **69–71**, **90–92**, *91–92*
security scopes, **783**, *783*
software updates, **369–371**
Off-Peak Synchronization Frequency option, 754
Office of Government Commerce (OGC), 2
Offline Files screen, 652, *653*
offline image servicing, **520–522**, *521–522*
Only The Instances Of The Objects That Are Assigned To The Specified Security Scopes Or Collections option, 786
Only When A User Is Logged On option, 329
Only When No User Is Logged On option, 329
Operate phase for MOF, **10**
operating system deployment (OSD), **15**, **451**
bare metal, 452, **492–497**, *492*, *494*
device drivers, **497–499**, *497–499*
distribution points, **455**
driver catalogs, **459**
enhancements, **19**
images, **455–456**
automatic building and capturing, **477–480**, *478–480*
boot. *See* boot images
deploying, **482–483**
reference computers, **480–481**, *481–482*
installers, **456**
legacy boot images, **522–523**
MDT, **510–516**, *511–513*, *515*
migration objects, **76–77**
Network Access account, **461–462**, *462*
new features, **451–452**
offline image servicing, **520–522**, *521–522*
process, **460**
PXE on distribution points, **464–465**, *465*
scenarios, **452**
source, **468–470**, *469–470*
state migration points, 455, **462–464**, *463*
task sequences, **457–459**
for capture image, **471–476**, *472–477*
deploying, **487–491**, *488–491*
developing, **483–486**, *484–486*
user device affinity, **459**, **500–503**, *500–503*
user state maintenance, **524**, *524*
virtual hard drives, **516–519**, ***518–520***
Windows To Go, **504–510**, *504–509*
Operating System Deployment Manager role, 600
operating systems
client requirements, **25–31**
client support, **232–234**
mobile device management, **703–704**
P2V Migration Toolkit requirements, 112
report, 591
server requirements, **32–36**
Operations Administrator role, 600, 776
Operations Manager Alerts option, 433
operations phase, **11**
Operations System Deployment Manager option, 776
Option tab for group discovery, 240, *241*
optional application information, **313–314**
Optional Components tab, boot images, 454
Options tab for Software Center, 342, *342*
ORDER BY keyword, 612
Organization Name setting, 230, 391
organizational units (OUs), **236**
orphaned packages, 855
out-of-band management, **17–18**, 25, 591
out-of-band service point role, 47, **191–192**, *192–193*
outboundcontentmanager.log file, 772
overlapping boundaries, 45
Owners option, 320

P

P2V Migration Toolkit, **111–112**
non-task sequences, **116–119**, *117*
requirements, **112**
scenarios, **112–113**
steps, **113–117**, *114–117*
task sequences, **113**
Package Conversion Dashboard, 105, *106*, 111
Package Conversion Manager, **103–104**, *104*
Package Conversion Wizard, 107–108, *109*
Package Source setting, **425**
packages
deployment, **372–373**, 424–427
library, 42
migrating, **103**
best practices, **110**
monitoring, **110–111**, *111*
Package Conversion Manager, **103–104**, *104*
process, **104–110**, *106*, *108–109*
orphaned, 855
Windows To Go, **506–507**, *507*
Packages node, 291, *292*
PackageScanReport.XML file, 111, *111*
parameters for reports, **603**
partner software updates catalogs, **438–439**, *439*
Password Complexity option, 711, 745
Password Expiration In Days option, 711
Password Never Expires property, 731

Password page, **744–745**, *744*
Password Quality option, 745
Password Settings window, **709–710**, *710*
passwords
  change requirements, **731**
  mobile devices, **709–710**, *710*, **744–745**, *744*
Patch property, 249
Patch Tuesday, **374–376**, *375*
paths, discovery, **236**
PCMTrace.log file, 111
PDP And IMAP Email option, 748
Peak Synchronization Frequency option, 754
Peak Synchronization page, 754, *755*
Pending state in Asset Intelligence, 569
Period Of Time For Which All Pending Deployments With Deadline setting, 398
permissions
  Application Administrator, *777*, *777*
  central administration sites, 135
  clients, 230
  Configuration Manager deployment, 845
  reports, **596–597**, *597*, 601
  Software Update Manager, **393–394**
Persist Content In The Client Cache option, **325**
personal devices, mobile devices wipe vs. selective wipes, **769**
Personal Wallet Software While Locked option, 747
.pfx files, 215, 222
phases in client installation, **266**
Photo Synchronization option, 753
physical locations, **57**
physical-to-virtual Migration Toolkit. *See* P2V Migration Toolkit
PkgLib folder, 174–175, *175*
PkgXferMgr component, 43
PKI certificates, 262–263
Plan phase for MOF, **9–10**
"Planning for Site Systems in Configuration Management" document, 133
Platform page for Windows Intune, 734–735, *734*
Platform Applicability page, 761–762, *762*
Plug-ins option, 749
POC (proof-of-concept) environments, **60–61**
policies
  endpoint protection, **679**
    antimalware, **679–685**, *680–685*
    assigning, **687**, *687*
    Windows Firewall, **685–686**, *686*
  group
    client installation, **257**
    SCEP, 673
    settings, **393**
Policy Polling Interval (Minutes) setting, 391
Policy Spy tool, 858, *858*
Polling Schedule tab, 242–243, *243*
POP And IMAP Email option, 712
Pop-up Blocker option, 749
Port Number setting, 717
portalwebMSI file, 199
portlctl.log file, 199
ports
  proxy points, 717
  WSUS, 411, *412*
post-installation phase in client installation, 266
post-migration considerations, **101–102**
post-recovery tasks, **821–822**, *822*
power control in out-of-band management, **17**
power management
  centralized, **19**
  client setting, 232
  report, 591
Power Viewer Tool, 858, *859*
PowerShell
  application information, **314**
  software update points, 410
PowerShell Execution Policy option, 231
pre-deploying user applications, 503, *503*
pre-installation phase in client installation, 266
preinst.exe tool, **820–821**
premigration in package conversions, 110
PREREQCHK.EXE.file, 126
Prerequisite Check page, 134, *134*, 815, *815*
Prerequisite Components page, 813–814, *813*
Prerequisites Downloads page, 130–131, *130*
Prerequisites Licenses page, 130
PrestageContent.log file, 98
prestaged content, **43**, **294**, **316**, *316*
prestaged media, 459, **504–506**, *504–506*
Primary Computer Users report, 565
Primary Site Installation page, 138
primary sites, **39–40**
  recovering, 817
  servers, **122**
    checklist, **127**
    implementing, **136–140**, *137–140*
  software update points, **381–382**
    child of CAS, **407–408**, *409*
    stand-alone, **410–413**, *412*
priorities
  application deployment type, 323
  policies, 687, *687*
  software update distribution, **425**
Privacy URL option, 321
private firewall profiles, 686
problem management, **6–7**, **11**
processing options for reports, **606–607**
processor requirements for clients, 25
Product Code option, 327
Product Key page, 130, *130*
products in updates, **386–387**
Products page
  Software Update Point role, 207, *208*
  software updates, 415, *416*
  third-party updates, 443, *444*
Profile Settings screen, 655, *656*
profiles
  certificate, **656–660**, *657–660*
  remote, **654–656**, *655–656*
  user, **650–654**, *651–654*
  VPN, **660–663**, *661–664*
  Wi-Fi, **665–667**, *665–668*
  Windows Firewall policies, 686

Programs tab, **327**, *327*
proof-of-concept (POC) environments, **60–61**
Properties dialog box for applications, 319
Properties Of New Template dialog box, 219
protection, endpoint. *See* System Center Endpoint Protection (SCEP)
providers in hardware inventory, **540**
provisioned systems, 191
provisioning
  command lines, **252**
  workstations, 17–18
Proxy and Account Settings page, 204, *204*
proxy management points, **180–181**
proxy settings, 437
  Asset Intelligence, 577–578
  software updates, 385
  VPN profiles, 663, *663*
  Wi-Fi profiles, 667
public firewall profiles, 686
publishing updates. *See* System Center Updates Publisher (SCUP)
Pull Distribution Point page, 169–170, *169*
Purpose setting in application deployment, 336
push client installation, **253–256**, *255–257*
PXE and PXE page
  boot images for, **467–468**, *467*
  capture images for, **471–474**, *472–474*
  configuring, **42**
  distribution points, 170, *170*, **464–465**, *465*
  unknown computer support, 495, *495*
PXE Settings page, 170, *170*

Q

queries, **13–14**, **182**
Query Rule for collections, 784
queues
  CEViewer, **853**, *853*
  DP Job Manager, **852**, *852*
quick antimalware scans, 680

R

RAM requirements for clients, 25
Ratings Region option, 752
RBA viewer, **793–795**, *794–795*, 855, *856*
RBAC (Role-Based Access Control) model, 773
RCMCtrl.log file, 848–849, *849*
Read-only Analyst role, 600, *776*
Real-Time Protection page, 682, *682*
Reassign Shared Distribution Point wizard, 93–94, *94*
reassigning distribution points, **85**
recovery. *See* disaster recovery
Recursively Search Active Directory Child Containers option, 237
reference computer images, **480–481**, *481–482*
References tab for sample application, 321
refresh computer deployment scenario, 452
Refresh Interval (Hours) option, 709
Registry
  64 bit applications, 634
  hardware inventory, **541–542**
  Report Builder, 614
  site installation validation, **148–149**, *149–150*
Release and Deployment Management process, **8**
remediation, client, **266–267**, *267*
reminders for client software updates, 391
remote connection profiles, **654–656**, *655–656*
remote console for out-of-band management, 18
remote control, **16**
remote distribution point throttling, **294**
remote installation, **128**
Remote Tools Operator role, 601, *776*
Remote Tools option for clients, 232
Removable Storage option, 754
Remove-CMSoftwareUpdatePoint command, 410
Repeated Malware Detection alerts, 690
repeating services point role, 47
Replace Hardware scenario, 510, **515–516**
replication, 50
  SQL, **307**
  troubleshooting, **845–849**, *846*, *848–849*
replication traffic reports, 591
Report Builder, **613–616**, *615*
Report Manager, **594–595**, *595*
Reporting Services point, **193–194**, *194*
Reporting Services Point page, 586, *587*
reporting services site system, **586–587**, *587*
reports, 16–17, 583–584
  Asset Intelligence, **571–575**
  BIDS, **616–618**
  client health, **287**, *288*
  client inventory, **547**
  Compliance Settings, **646–647**
  creating, **611–618**, *615*
  exporting, **621**
  hardware inventory, **530–532**
  importing, **603**, **620–621**
  linked, **619**
  logos, 595–596, *596*
  managing, **601–608**
  migrating, **78–79**
  migration results, **85**
  models, **613**
  moving, **619**
  Report Builder, **613–616**, *615*
  Reporting Services, **193–194**, *194*
  running, **593–595**, *594–595*
  SCEP, **693–695**, 694–695
  security, **596–601**, *597*, 608
  software metering, **560**, **562**, **564**, 592
  software updates, **420–421**, *421*, **448–449**
  SQL commands, **611–612**
  SQL Reporting Services, **19**
  SQL Server Reporting Services, **584–589**, *587*, *589*
  status messages, **840–841**
  subscriptions, **604–605**, **609–611**, *610*
Require Administrator Approval If Users Request This Application option, 336
Require Email Encryption/Encryption Algorithm option, *757*

Require Email Signing/Signing Algorithm option, *757*
Require Password Settings On Mobile Devices option, *710*, *744–745*
Require The Site Server To Initiate Connections To This Site System option, *403*, *408*, *411*
Required Components to Use Administration UI page, *402*
requirements and Requirements tab
  Application Catalog Web Service Point, *198*
  Application Catalog Web Site Point, *198*
  application deployment, **297–298**, **346–347**, *349*
  application information, **331–332**, *331*
  Asset Intelligence, **563–566**, **568**
  clients, **24–32**
  cloud integration, **214**
  distribution points, **177**
  Endpoint Protection points, *210*
  fallback status points, *190*
  management certificates, **215**
  management points, **183**
  mobile devices, *202*
  Reporting Services, *195*
  servers, **32–36**
  site servers, **125–127**
  Software Update Point role, *208*
  state migration points, *189*
  system health validator points, *186*
RESETKEYINFORMATION property, *250*
Resource Explorer, **535–536**, *535*, **545–546**, *546*, *549*, **550**
resources
  discovery. *See* discovering resources
  for security scopes, **781–782**, *782*
Resources folder, *589*
Restart Countdown setting, *388*
restoring backups, **807–810**, *809*
Retain Client Status History For The Following Number Of Days setting, *286*
Retire/Reinstate option, **317**
Retries/Retry Delay (Minutes/Renewal Threshold (%) option, *764*
/retry property, *248*
return codes, **298**, *332*, *332*
Return Codes tab, *332*, *332*
review phase in migration, *82*
Review Required Ports For PXE dialog box, *465*, *465*
Revision History option, **315**, *315*
Ribbon options, **314–319**, *315–318*
risk, *12*
roaming
  global, *37*
  mobile device settings, *754*, *755*
  site system roles, *161*
Roaming page, *754*, *755*
Roaming Profiles screen, *653*, *653*
roaming user profiles, *651*, *653*, *653*
Role-Based Access Control (RBAC) model, *773*
role-based administration, **53–54**, **773**
  administrative users, **785**, *786*, **789–790**
  collections, **784–785**, **789–790**
  overview, **773–774**
  RBA viewer, **793–795**, *794–795*
  security
    roles, **774–778**, *775*, *777*, *787*
    scopes, **778–783**, *778–779*, *782–783*, **787–792**, *787–792*
  software updates, **393–394**
Role-Based Administration Modeling and Auditing tool, *793*, *855*, *856*
Role Services page, *399*
roles
  mobile devices, **715–716**
    Application Catalog web service point, **720**, *721*
    distribution point, **720**, *720*
    enrollment point, **717–718**, *717*
    enrollment proxy point, **716–717**, *716*
    management point, **718–719**, *718*
    Microsoft enterprise certification authority, **719**, *719*
  site system. *See* site system roles
Root CA Certificate option, *765*
-rootcerts property, *262*
-rootkeypath property, *261*
rules
  application deployment, **346–347**
  collections, **784**
  configuration baselines, *631*, **640–644**, *641*, *645*
  configuration items, **634–638**, *635*, *637–638*
  software metering
    adding, **556–558**, *557*
    Automatic Rule Generation, **554–555**, *555*
    enabling and disabling, **555–556**
    migrating, **78**
  software updates, **364**, *371*, **374–376**, *375*
  supersedence, **385–386**
  System Center Updates Publisher, *395*, **440–441**, *441*
Run Installation and Uninstall Programs in 32-Bit Process on 64-Bit Clients option, *327*
Run Metering Summarization Tool, *855*, *856*
Run Task As Soon As Possible After A Scheduled Start Is Missed option, *278*
running reports, **593–595**, *594–595*

S

Scan Settings page, *681*, *681*
scans
  antimalware policy, **679–681**, *680–681*
  software updates, **397**
SCCMContentLib folder, *174*, *174*
SCCMContentLib library, *42*
SCEP. *See* System Center Endpoint Protection (SCEP)
SCEP Enrollment page, *763*, *763*
SCEPInstall.exe utility, *675*
Schedule Deployment Re-evaluation setting, **398**
Schedule Evaluation setting, *429*
Schedule Updates Wizard, *520*, *521*
Scheduled Scans option, *680–681*, *680*

scheduled tasks
Actions page, **275**, *276*
CCMEval, **279–283**, *279*, *282*
client health, **274–275**, *274–275*
Conditions page, **276**, *277*
History page, 278, *278*
Settings page, **277–278**, *277*
Triggers page, **275**, *276*
schedules
antimalware scans, 680–681, *680–681*
application deployment, 337, *337*
content distribution, **42**
deployment templates, 371
discovery, **242–243**, *243–244*, 707
inventory, **536–537**
report subscriptions, 609
software updates
deployments, 429–430, *430*
scans, **397**
synchronization, 377, **385**, 417, *417*
Scheduling page
Deploy Software Updates Wizard, 429–430, *430*
Deploy Software Wizard, 337, *337*
schema for Active Directory, **37–38**
scheme extensions, 134
scopes, security, 53, **778**, *778*
applications, **319**
creating, **779–781**, *779*
resources, **781–782**, *782*
scenario, **787–792**, *787–792*
viewing, **783**, *783*
Scratch Space setting, 512
Screen Capture option, 746
scripts for client installation, **258**
SCUP (System Center Updates Publisher), **800**
SCW (Security Configuration Wizard), **853**, *854*
search folders in migration, **78**
search options for software updates, **421–423**, *422–423*
secondary site servers
implementing, **140–147**, *141–147*
overview, **122–123**
secondary sites, **40–41**
migrating, 86
recovering, **818**
upgrading, **98**, *98*
security
mobile devices, **712–713**, *713*, 753–754, *753*
reports, **596–601**, *597*, 608
roles, 53, **774–778**, *775*, *777*, 787
SCEP, **670–672**
scopes, 53, **778**, *778*
applications, **319**
creating, **779–781**, *779*
resources, **781–782**, *782*
scenario, **787–792**, *787–792*
viewing, **783**, *783*
sites, **51**
SQL Server Reporting Services, **586**
Security Administrator role, 601, *776*
Security Compliance Manager, **647–648**, *648*
Security Configuration page
mobile devices, 768, *769*
Wi-Fi profiles, 665, *666*
Security Configuration Wizard (SCW), **853**, *854*
Security Level For Internet Zone option, 751
Security Level For Intranet Zone option, 751
Security Level For Restricted Sites Zone option, 751
Security Level For Trusted Sites Zone option, 751
Security page
application, **323**
boot images, 454
mobile devices, 753–754, *753*
operating system images, 456
operating system installers, 456
unknown computer support, 496, *496*
Security Settings window, **712–713**, *713*
Security Warning window, 439, *440*
Select Application page, 505, *505*
SELECT command for reports, 612
Select Deployment Package option, 425
Select Deployment Template option, 428
Select Files page, 649, *649*
Select Media Type page, 475, *475*, 496, *496*
Select New Container dialog box, 235, *236*
Selected Language option, 321
selective wipe, **769–771**, *770–771*
Self-Update option, **393**
Send Password Recovery PIN To Exchange Server option, 745
Send Schedule Tool, 858, *859*
server-based tools for troubleshooting, **852–856**, *852–856*
Server Deployment scenario, 510
Server Language Selection page, 131
server locator point functionality, **182**
servers
requirements, **32–36**
setting migration, 66
site. *See* site servers
Service Asset and Configuration Management (SACM) process, **7**
service certificates
requesting and exporting, **220–221**, *220*
templates, **219–220**, *219*
Service Design phase, **3–4**
service desk function, **5**
Service-Level Agreements (SLAs), 6
Service Level Management (SLM) process, **8**
Service Lifecycle, 2
Service Management Functions (SMFs), **9–12**
service management overview, **1**
ITIL, **2–9**
MOF, **9–12**
service monitoring and control, **11**
Service Operation phase, **3–5**
/Service property, 248
Service Strategy phase, **3–4**
Service Transition phase, 3, **5**
service validation, **153**, *154*
Services registry key, 149, *150*
Servicing tab, 456, 522, *522*
Set-CMSoftwareUpdatePoint command, 382
Set-MsolUser command, 731
Set Security Scope option, **319**
Set Security Scopes window, 781–782

Set The Mobile Device Management Authority screen, 731, *732*
Setting Summary page, 133–134, *133*
settings and Settings page
Add Exchange Server Wizard, **708**
Application Settings, **713**, *714*
Email Management Settings, **711–712**, *711*
General Settings, **709**, *709*
Password Settings, **709–710**, *710*
Security Settings, **712–713**, *713*
Application Deployment, **299**
migrating, **77–78**
recovery process, 815, *815*
scheduled tasks, **277–278**, *277*
task sequences, 458
Settings Management feature, **16**
Settings Summary page, 815, *815*
Settings Synchronization option, 753
Settings Synchronization Over Metered Connections option, 753
Setup Wizard
central administration sites, **129–134**, *129–134*
primary site servers, **136–140**, *137–140*
System Center Updates Publisher, 436, *436*
Show Install Status option, 147, *147*
Show Message menu, 839, *839*
Show Notifications For New Deployments option, 231
side-by-side migration, **83**
clients, **98–99**
configuring, **86–88**, *87*
distribution points, **88–89**, **93–98**, *94–95*, *97*
process, **83–86**, *84*
secondary sites, **98**, *98*
sign-in page for Windows Intune, 732, *732*
-signcertpath property, 262
Signing And Encryption tab, 547
Simple Schedule option, 538
Simulate Application Deployment Wizard, 317, *317*
Simulate Deployment option, **317**, *317*
Single Computer page, 492, *492*, 515
single instance storage, **293**
Site and Installation Settings page, 131, *131*, 814, *814*
site data, 847, *848*
site database server point role, 47
Site Maintenance dialog box, 558–559, *559*
Site Recovery Information page, 812, *813*
Site Repair Wizard, 811
Site reports, 591
Site Server and Database Recovery Options page, 812, *812*
site servers
backing up, **805–806**, *806*
checklist, **126–127**
cloud communication, **215**
implementing, **125**, *125*
central administration, **127–136**, *129–135*
primary sites, **136–140**, *137–140*
secondary sites, **140–147**, *141–147*
software requirements, **125–127**
troubleshooting, **154–157**, *155–156*, *158*
unattended installation, **157–159**
inventory, **551**
log files, **832–834**
primary, **122**
secondary, **122–123**
verifying, **147–153**, *148*
database validation, **153**, *154*
file system validation, **150**, *151*
group validation, **151–152**, *152*
registry validation, **148–149**, *149–150*
services validation, **153**, *154*
WMI validation, **153**, *153*
Site Settings Properties dialog box, 270–271, *270*
Site Status dashboard, 838, *839*
Site System Installation Account setting, 404, 408, 411
site system roles, **45–47**
Application Catalog Web Service Point, **195–199**, *196–198*
Application Catalog Web Site Point, **195–199**, *196–198*
Asset Intelligence Synchronization Point, **210–211**, *211*
component servers, **165**
configuring, 139, *140*
distribution points, **165–176**, *166–176*
Endpoint Protection Point, **209–210**, *209*
fallback status points, **189–191**, *190*
installing, **160–163**, *161–162*
management points, **178–183**, *179–180*
mobile device and AMT enrollment point, **199–203**, *201–202*
out-of-band management, **191–192**, *192–193*
overview, **163–165**
Reporting Services point, **193–194**, *194*
site database servers, **184**
site servers, **183–184**
site systems, **184**
Software Update Point, **203–208**, *203–208*
state migration points, **186–189**, *186–188*
system health validator points, **184–185**
Site System Roles page, 139, *140*
site systems, **184**
backing up, **799**
design, **47–49**
planning, **58–59**
Site tab, 265, *265*
site-to-site communications, 308
-sitecode property, 260
sitecomp.log file, 165, 589, 772
sites, **38**, *38*
boundaries, **44–45**
central administration, **38–39**
communications, **50**
databases, 47, **823–824**, *824*
distribution points, **41–44**, *44*

failure effects, **808–809**
maintenance tasks, 829–830
migrating, *67*
primary, **39–40**
recovering, **809–810**, *809*, **817–819**
secondary, **40–41**
security, **51**
types, **122–123**, *124*
upgrading, **98**, *98*
64 bit applications, Registry, 634
Size Limit (KB) For Email Attachments (Automatically Downloaded) setting, 712
Size Limit (KB) For HTML Email (Automatically Downloaded) setting, 712
Size Limit (KB) For Plain Text Email (Automatically Downloaded) setting, 712
skpswi.dat file, 547–548
SLAs (Service-Level Agreements), 6
SLM (Service Level Management) process, **8**
SmartScreen option, 760
SMFs (Service Management Functions), **9–12**
smp.msi file, 189
smpmsi.log file, 189
SMS And MMS Messaging option, 713, 754
SMS_CCM folder, 150, *151*
SMS Database Monitor, 157
sms_def.mof file, 79, 529
SMS_Executive component, 155–156, *155*
SMS provider point role, 47
SMS Provider Settings page, **132–133**
SMS providers
high availability, 49
purpose, **157**
settings, **132–133**
SMS registry key, 148
smsawebsvcsetup.log file, 198
smsbkup.ctl file, 801, *801*
smsbkup.log file, 801, 807
SMSCacheDir property, 250
SMSCacheFlags property, **250–251**
SMSCacheSize property, 251
SMSConfigSource property, 251
smsdbmon.log file, 157, 184
SMSDIRECTORYLOOKUP property, 251
SMSDPPROV.LOG file, 94
Smsenrollsrvsetup.log file, 202
Smsenrollwebsetup.log file, 202
smsexec.log file, 156, *156*
SMSFSPSetup.log file, 191
SMSMP property, 251
smsportwebsetup.log file, 198
smsprov.log file, 184
SMSPUBLICROOTKEY property, 249
smspxe.log file, 465
SMSROOTKEYPATH property, 249
SMSSiteCode property, 251
smssmpsetup.log file, 189
snapshots
archiving, **802–803**, *803*
report properties, 608
Software Available Time setting, 430
software categories for Asset Intelligence, **566–567**
Software Center
application deployment, 339–342, *341–342*
distribution points, **295**
software updates, 365, *365*
Software Deployment option, 232
Software Deployment page, 304, *305*
software distribution
client installation, **258**
collections. *See* collections
distribution points. *See* distribution points
packages. *See* packages
reports, 591
Software Distribution Component Properties dialog box, **306–307**, *307*
Software Download While Roaming option, 754
software families for Asset Intelligence, **567**
Software Install Program Might Force A Device Restart option, 331
software inventory
clients, 232
collecting, **533–535**, *534*
configuring, **542–550**, *543–545*
Software Inventory During The Following Days setting, 286
software licenses for Asset Intelligence, **578–581**, *578*, *580*
Software Metering Client Agent, 553, 564
Software Metering feature, **15**, **553**
clients, **560**, *561*
configuring, **553–554**, *554*
maintenance tasks, **558–560**, *559*
overview, **553**
reports, **560**, **562**, **564**, 592
rules
adding, **556–558**, *557*
Automatic Rule Generation, **554–555**, *555*
enabling and disabling, **555–556**
migrating, **78**
Software Metering option, 232
Software Metering Properties dialog box, 554–555, *555*
Software Metering Summarization Progress report, 559, *559*
Software Metering Usage Report Cycle action, 560, *561*
software reports, **573–574**
software requirements
Application Catalog Web Service Point, 198
Application Catalog Web Site Point, 198
Asset Intelligence Synchronization Point, 210
distribution points, **177**
Endpoint Protection points, 210
fallback status points, 190
management points, **183**
mobile device and AMT enrollment point role, 202
Reporting Services, 195
servers, **36**
site servers, **125–127**
Software Update Point role, 208
state migration points, 189
system health validator points, 186
Software Update Catalog, 394
Software Update Manager role, 776
reports, 601
software updates, **393–394**

software update point role, 47
  active, **413**
  infrastructure, **380–382**
  install planning, **382–384**
  settings, **203–208**, *203–208*
  software updates, **367–368**
  testing, **396**
software update points
  Central Administration Site, **403–407**, *404–406*
  general settings, **384–385**
  primary sites
    child of CAS, **407–408**, *409*
    stand-alone, **410–413**, *412*
  synchronization, **385–387**
Software Update Scan Schedule setting, **397**
Software Update/Software Update Group option, 428
software updates, **14–15**, **363**
  classifications
    classes, **386**
    configuring, 415, *415*
    metadata, 369
  client installation, **257**
  client settings, **392**, *392*
  compliance, **377–378**
  Computer Client Agent, **390–391**, *390*
  deployments, **373–374**, **378–380**
    Deploy Software Updates Wizard, **427–434**, *429–432*
    packages, **372–373**
    rules, **374–376**, *375*
    templates, **371–372**
  downloading, **424–427**
  enabling, 232
  files, **369**
  finding, **420–423**, *421–423*
  goals, **380**
  group policy settings, **393**
  groups, **364**, 370, **427**
  languages, **387**, 415, *416*, 434
  maintenance windows, **387–389**, *388*
  metadata, **368–369**, 414, 419
  migrating, **76**
  monitoring, **445–449**, *445–448*
  new features, **364–366**, *365*
  objects, **369–371**
  planning, **380**
  prerequisites, **366–367**
  process, **376**
  products, **386–387**
  properties, **389–390**
  reports, **420–421**, *421*, 592
  role-based administration, **393–394**
  settings, **414–417**, *415–418*
  software update point role. *See* software update point role
  Software Updates Agent, **368**
  Software Updates Client Agent, *397*
  summary details, **387**
  supersedence rules, **385–386**
  synchronization, **376–377**, **414–417**, *415–418*
  System Center Updates Publisher, **394–395**
  templates, **366**, **371–372**
  test labs, **395–396**
  update files, **387**
  Windows Server Update Services Server
    console, **402**
    installation, **398–401**
Software Updates Client Agent, **396–398**, *397*
Software Updates Deployment Evaluation Cycle action, 392
Software Updates Scan Cycle action, 392
sorting reports, 612
source hierarchy, **67–68**, *67*, 86
/source property, 247
source sites, migrating, 67
Specify An FQDN For This Site System For Use On The Internet option, 403, 407
Specify An FQDN For This Site System On The Intranet option, 410
Specify Intranet Microsoft Update Service Location option, **393**
Specify Microsoft Active Protection Service window, 674
Specify Peak Time option, 754
Specify Sideloading Key dialog box, 351, *351*
Specify The Content Destination page, 467
speed of networks, 45
splash.hta file, 129
SpyNet, **670–671**
SQL
  considerations, **49–50**
  memory, 128, 135
  replication, **307**
  reports
    commands, **611–612**
    SQL Reporting Services, **19**, **799–800**
SQL Server Management Studio, 585
SQL Server Reporting Services (SSRS), 193–194, **584–589**, *587*, *589*
SQL Server Settings page, 143, *143*
srsrp.log file, 195, 589
srsrpMSI.log file, 195, 589
srsrpsetup.log file, 195
SSRS (SQL Server Reporting Services), 193–194, **584–589**, *587*, *589*
stand-alone media for task sequences, 459
stand-alone primary sites for software update points, 381
standalone site recovery, 817
state-based distribution point groups, **43**
State Message Reporting Cycle (Minutes) setting, 391
State Messaging setting, 232
State Migration page, 485, *485*, 494, *494*
State Migration Point page, 187–188, *187*, **462–464**, *463*
state migration point role, 47
state migration points
  configuring, **462–464**, *463*
  operating system deployment, 455
State Migration report, 592
states
  Asset Intelligence validation, **563**
  link, **846**
statistics for in-console monitoring, **445–448**, *445–448*
Status Message Details dialog box, 839, *840*
status messages, **837–839**, *839–840*
  default reports, 592
  deployment, **841–842**
  distribution, **843**

distribution point configuration, **844**
distribution point groups, **844**
system, **844–845**
web reports, **840–841**
Status Messages During The Following Days setting, 286
Stop Data Gathering dialog box, 102
Stop The Task If It Takes Longer Than setting, 278
Storage Card Encryption option, 713, 756
Storage Folder Settings page, 462, *463*
Store page, 747–748, *748*
Style folder for reports, 589
Subject Alternative Name option, 765
Subject Name Format option, 765
Subscription Schedule page, 609
subscriptions
reports, **604–605**, **609–611**, *610*
Windows Intune, 728
summarization tasks for software metering, **559**
Summarize Installed Software Data task, 564
Summary Details information for software updates, **387**
Summary page, 736
Asset Intelligence, 578
certificate profiles, 660
client health, 283, *284*
computer information, 493
configuration items, 638, *638*
Deploy Software Updates Wizard, 434, *435*
device drivers, 499
distribution points, 173
image capture, 481
Microsoft Deployment Toolkit, 516
mobile devices, 714, 765
remote profiles, 656
secondary site servers, 145, *146*
task sequences, 477, 486
user profiles, 653, *653*
VPN profiles, 663
Wi-Fi profiles, 667
superseded software updates, **365**
supersedence, 378
application deployment, **343–344**, *344–345*
Application References, **296**
software updates, **385–386**
Supersedence page for applications, **323**, *323*
Supersedence Rules page
Software Update Point role, 206, *206*
software updates, 415, *417*
Supported Platforms page, 658, *659*, 761, *761*
VPN profiles, 663, *664*
Wi-Fi profiles, 667, *668*
Supports Contacts option, 320
Suppress Any Required Computer Restart After The Endpoint Protection Client Is Installed option, 231
Supsetup.log file, 208
Suspend BitLocker PIN Entry Or Restart option, 230
swmproc.log file, 560
SWMTRReportGen.log file, 560
Sync Schedule tab, 417, *418*
synchronization
Asset Intelligence, **569–571**, **576–578**, *577*
discovery, 707
mobile devices, 754, *755*
monitoring, **448**, *448*
software update points, 405–406, 412
software updates, **376–377**, **385–387**, **414–417**, *415–418*
Windows Azure Active Directory, **730**, *730*
Synchronization Point Schedule page, 578
Synchronization Schedule page
Asset Intelligence Synchronization Point, 210
Software Update Point role, 205
Synchronization Source page, 204–205, *205*
Synchronize From An Upstream Data Source Location (URL) option, 405, 412
Synchronize From Microsoft Update option, 405, 412
System Center Endpoint Protection (SCEP), **19–20**, **669**
alerts, **690–691**, *691–692*
benefits, **670–672**
definition files, **687–690**, *688–689*
Endpoint Protection client agent, **675–679**, *676–677*
Endpoint Protection Point role, **672–675**, *674*
endpoint protection policies, **679**
antimalware, **679–685**, *680–685*
assigning, **687**, *687*
Windows Firewall, **685–686**, *686*
vs. FEP, **669**
malware scenario, **695–699**, *696–698*
reporting, **693–695**, 694–695
settings, **231**
System Center Online service, 566
System Center Updates Publisher (SCUP), 129, **376**, **436**
backups, **800**
components, **394–395**
configuring, **436–437**, *437–438*
importing updates, **439**, *440*
installing, **436**, *436*
partner software updates catalogs, **438–439**, *439*
publishing updates, **442–443**, *442*
rules, **440–441**, *441*
third-party updates, **443–445**, *444*
system discovery, 52, **239**, *239*
system health validator point role, 47, **184–185**
system requirements
client, **24–32**
servers, **32–36**
System Center Updates Publisher, **395**
System Restart Turnaround Time setting, 388
system role. *See* site system roles
System Role Selection page
Asset Intelligence, 578
reporting site role, 586
state migration points, 462, *463*
System Security page, 759–760, *759*
system status messages, **844–845**

system updates. *See* System Center Updates Publisher (SCUP)

T

Task Sequence Designer, 114, *115*
Task Sequence Information page, 483, 493
task sequences
  BitLocker, **507–508**, *508*
  capture images, **471–476**, *472–477*
  deploying, **487–491**, *488–491*
  developing, **483–486**, *484–486*
  MDT, **513–515**, *513*, *515*
  media boot, **475–476**, *475–477*
  operating system deployment, **457–459**, **493–494**, *494*
  P2V Migration Toolkit, **113–117**, *114–117*
  prestaged media, **504–506**, *504–506*
  reports, 592
  virtual hard drives, **517–518**
Technical Management function, **6**
Technology setting, 325
templates
  service certificates, **219–220**, *219*
  software updates, **366**, **371–372**
test labs, **395–396**
test phase in migration, 82
testing
  site backups, **806–807**, *806*
  software update points, **396**
thin images, 460
third-party updates, **443–445**, *444*
Threat Overrides page, 684, *684*
thresholds for alerts, 691, *692*
throttling
  content distribution, **42**
  remote distribution point, **294**
time stamps for log files, **361**
timing in troubleshooting, 845
Trace Log tool, 224
Trace32 utility, 157
Triggers page, **275**, *276*
troubleshooting, **827**
  Application Catalog Web Service Point, **198–199**
  Application Catalog Web Site Point, **198–199**
  application deployment, **358–361**, *359–360*
  Asset Intelligence Synchronization Point, **211**
  backups, **807**
  client-based tools, **856–859**, *857–860*
  client installation, **266**
  component servers, **165**
  Configuration Manager deployment, **845**
  Database Replication, **845–849**, *846*, *848–849*
  distribution points, **177**, *177*
  Endpoint Protection points, 210
  enrollment proxy point and enrollment point, **202–203**
  fallback status points, 191
  inventory, **550–552**
  log files for, **832–837**
  maintenance plans for, **827–831**, *828*
  management points, **183**
  mobile devices, **771–772**
  Reporting Services, **195**
  scenario, **850–852**
  server-based tools, **852–856**, *852–856*
  site database servers, **184**
  site servers, **154–157**, *155–156*, *158*
  Software Update Point role, **208**
  state migration points, **189**
  status messages for, **837–845**, *839–840*
Trusted CA Certificate screen, 658, *659*
Trusted Publishers option, 437
Trusted Root CA Certificate page, 762, *763*
TV Show Rating option, 752
Type of Deployment setting, 428

U

unattended site recovery, **818–819**
unattended site server installation, **157–159**
Uncategorized state in Asset Intelligence, 569
Uninstall Program option, 327
/Uninstall property, 248
Uninstall Start In option, 327
Unix operating system
  application deployment, **354–355**, *354*
  client installation, **259–262**, *260*
  client support, 234
  support for, **30–32**
unknown computer support, **495–497**, *495–496*
Unknown package conversion state, 105
Unknown status in monitoring, 446
unmanaged scenarios, SCEP in, **672–673**
Unsigned Applications option, 713, *754*
Unsigned File Installation option, 713, 754
Update Files setting, **387**
Update lists feature, 366
Update Server option, 437
Updateable state in Asset Intelligence, 569
Updated Prerequisite Components page, 138
updates
  security, **687–690**, *688–689*
  software. *See* software updates
Updates option, 760
Upgrade Assessment report, 592
upgrading
  administrative console, 86
  clients, **270–271**, *270*
  Configuration Manager console, **100–101**
  distribution points, **93–98**, *94–95*, *97*
  secondary sites, **98**, *98*
uploading management certificates, **222**, *222*
UPN suffixes for Windows Intune, **728–729**, *729–730*
Use Default Distribution Point Groups Associated To This Collection option, **334–335**
Use Wake-On-LAN to Wake up Clients for Required Deployment option, 429
UsePKICert property, 248, 261
User And Device Affinity settings, 232, 306, *306*
User Categories option, 321
user-centric focus for distribution points, **295**
user configuration for mobile devices, **722–728**, *723–727*
user data, **650–654**, *651–654*

User Data and Profiles Health
report, 593
User-defined state in Asset
Intelligence, 568
User Device Affinity
application deployment,
355–358, *356–358*
configuring, **500–503**, *500–503*
operating system deployment,
459
report, 593
User Device Affinity Usage
Threshold (Days) setting, 502
User Device Affinity Usage
Threshold (Minutes) setting, 502
User Documentation option, 321
User-Driven Installation scenario,
510
User Experience settings
application deployment,
328–331, *329*
Deploy Software Updates
Wizard, 430, *431*
Deploy Software Wizard,
337–338, *337*
deployment templates, 371
software updates, 389
task sequence deployment, 489
visual experience, 431
user facing packages, 103
user state migration data, backing
up, 800
User State task category, 458
User To Accept Untrusted TLS
Certificates option, 760
User To Access Control option, 760
users
administrative, **785**, *786*,
789–790
discovery, 52, **240**
report, 593
state management, **524**, *524*

V

Validated state in Asset Intelligence,
568
validation
Asset Intelligence states,
568–569
configuration baseline rules,
644–646, *645*
configuration items, **634–638**,
635, *637–638*
content, **43**, *44*
databases, **153**, *154*
file systems, **150**, *151*
groups, **151–152**, *152*
registry, **148–149**, *149–150*
services, **153**, *154*
WMI, **153**, *153*
validator points, **184–185**
vendor updates, 395
verification
client installation, **265–266**,
265
site servers, **147–153**, *148*
database validation, **153**,
154
file system validation, **150**,
151
group validation, **151–152**,
152
Registry validation, **148–149**,
149–150
services validation, **153**, *154*
WMI validation, **153**, *153*
version setting for software
metering rules, 557
Video Chat Client option, 746
viewing
inventory information,
535–536, *535*
software inventory, **545–546**,
546, **549–550**
Virtual Application Name setting,
718
virtual application package
migration, **75**
Virtual Applications report, 593
virtual environments migration, 75
Virtual Environments That Contain
This Application option, 344
virtual hard drives, **516–517**
creating, **518–519**, *518–519*
managing, **519–522**, *520–522*
task sequences, **517–518**
Virus Protection option, 760
Virus Protection Signatures Are Up
To Date option, 760
Voice Assistant option, 746
Voice Assistant While Locked
option, 746
Voice Dialing option, 746
Voice Roaming option, 756
Volume Shadow Copy Service
(VSS), 797–798
VPN profiles, **660–663**, *661–664*

W

Wake on LAN feature
description, **16**
report, 593
Wakeup Spy tool, 859, *860*
WCM.log file, 208, 257
web applications, 355
web reports for status messages,
840–841
Web Site Name setting, 716
Website Name/Port Number
setting, 717–718
When Any Software Update
Deployment Deadline Is Reached
setting, 398
Whether Or Not A User Is Logged
On option, 329
Wi-Fi profiles
configuring, **665–667**, *665–668*
mobile devices, 767, *768*
wildcards in Compliance Settings,
634
Windows Azure Active Directory,
730–731, *730*
Windows Azure cloud services. *See*
cloud integration
Windows Azure Management
Portal, 222, 225
Windows Firewall policies,
685–686, *686*
Windows Intune, 47, **728**
connector, **731–737**, *732–737*
mobile device enrolling,
737–741, *738*, *740–742*
prerequisites, **728–730**, *729–730*
Windows Management
Instrumentation (WMI), **153**, *153*,
379
Windows operating system
client support, 232–234
event log settings, **565–566**
mobile device management,
703–704
Windows 7 support, **26–27**
Windows 8
application deployment,
350–352, *351*
support for, **27**
Windows Intune, **734–735**,
740–741, *741*
Windows Vista support, **26**
Windows XP support, **26**
Windows Phone devices, **735**

Windows RT VPN Profile option, *754*
Windows Server 2003 operating system support, **27–28**
Windows Server 2008 operating system support, **28**
Windows Server 2012 operating system support, **28–29**
Windows Server Update Services (WSUS), 15, 363
  central administration sites, 134
  console, **402**
  database backups, 800
  description, 366
  installing, **398–401**
  ports, 411, *412*
  reporting events, **385**
  software update points, 381–383
  Synchronization Manager, 376–377
Windows Server Work page, 760, *760*
Windows To Go, **504**
  creator packages, **506–507**, *507*
  running, **509–510**, *509*
  task sequences
    BitLocker, **507–508**, *508*
    prestaged media for, **504–506**, *504–506*
Windows Update Agent (WUA)
  compliance, 376–377
  event messages, 385
  software updates, 393
WinPE Creator Wizard, 117–118, *118*
wipe-and-load migration, **100**
wipe for mobile devices, **769–771**, *770–771*
Wireless Communications page, 757–758, *757*
Wireless Network Connection window, 757, *758*
Wireless Network Connections option, 713
Wizard Completed screen
  captured image, 483
  distribution points, 467
  task sequences, 477
WMI (Windows Management Instrumentation), **153**, *153*, 379
Work Information setting, 392
workspaces in Windows To Go, 509, *509*
workstations as distribution points, **293**
Write Filter Handling For Windows Embedded Devices option, 432
WSUS. *See* Windows Server Update Services (WSUS)
WSUSCtrl.log file, 208
wsusutil.exe utility, 76, **419**
WSYNCMGR.log file, 208
wtgcreator.exe command, 506
WUA (Windows Update Agent)
  compliance, 376–377
  event messages, 385
  software updates, 393